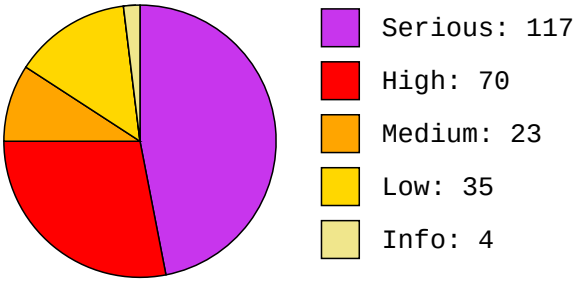
AlienVault: I.T Security Vulnerability Report

Job Name:	Scan Server	Scan time:	2015-06-10 17:41:15
Profile:	Default - Non destructive Full and Fast scan	Generated:	2015-06-10 17:46:01

Total number of vulnerabilities identified on 1 system(s)



Total number of vulnerabilities identified per system

HostIP	HostName	Serious	High	Med	Low	Info
10.47.30.102	Server2008	117	70	23	35	4

10.47.30.102	Server2008

Serious:

Microsoft Internet Explorer Remote Code Execution Vulnerability (2965111)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804441
Summary:
This host is missing a critical security update according to Microsoft
Bulletin MS14-021.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
The flaw exists in the way that Internet Explorer accesses an object in memory
that has been deleted or has not been properly allocated.
Impact:
Successful exploitation will allow attackers to corrupt memory by the
execution of arbitrary code in the context of the current user.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms14-021
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 415 $

Serious:

Microsoft .NET Framework Privilege Elevation Vulnerability (2958732)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804452
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS14-026.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
The flaw is due to the framework not properly restricting access to certain
application objects related to TypeFilterLevel checks.
Impact:
Successful exploitation could allow an attacker to bypass certain security
restrictions.
Impact Level: Application
Affected Software/OS:
Microsoft .NET Framework 1.1, 2.0, 3.5, 3.5.1, 4.0 and 4.5 and 4.5.1
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms14-026
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: Check for the version of vulnerable files
Version: $Revision: 758 $

Serious:

Microsoft Windows TCP/IP Remote Code Execution Vulnerability (2588516)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902484
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-083.
Vulnerability Insight:
The flaw is due to an integer overflow error in the TCP/IP
implementation when parsing UDP traffic and which can be exploited
via a continuous flow of specially crafted UDP datagrams sent to a
closed port.
Impact:
Successful exploitation could allow remote attacker to execute the arbitrary
code in kernel mode. An attacker could then install programs, view, change,
delete data or create new accounts with full user rights.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-083.mspx
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'tcpip.sys' file version
Version: $Revision: 13 $

Serious:

Microsoft Internet Explorer Multiple Use After Free Vulnerabilities (2817183)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903305
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS13-028.
Vulnerability Insight:
Unspecified use-after-free error occurs when dereference already freed
memory.
Impact:
Successful exploitation will allow attackers to execute arbitrary HTML or
script code in the context of the current user.
Impact Level: Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-028
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (c) 2013 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 11 $

Serious:

Microsoft Internet Explorer Multiple Use After Free Vulnerabilities (2829530)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903307
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS13-037.
Vulnerability Insight:
Multiple unspecified use-after-free error occurs when accessing already
freed memory.
Impact:
Successful exploitation will allow attackers to corrupt memory by the
execution of arbitrary code in the context of the current user and gain
access to potentially sensitive information stored in JSON data files.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-037
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (c) 2013 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 144 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2838727)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903309
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS13-047.
Vulnerability Insight:
Multiple unspecified error due to,
- Improper sanitation of user supplied input, when handling script debugging
for a specially crafted webpage.
- when improperly accesses an object in memory.
Impact:
Successful exploitation will allow attackers to corrupt memory by the
execution of arbitrary code in the context of the current user.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-047
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (c) 2013 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 11 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2846071)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903314
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS13-055.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Multiple unspecified error due to an,
- Improper handling of the encoding for Shift_JIS auto-selection.
- Improper handling of objects in memory.
Impact:
Successful exploitation will allow attackers to corrupt memory by the execution of arbitrary code in the context of the current user.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://technet.microsoft.com/en-us/security/bulletin/ms13-055
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 187 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2862772)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903315
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS13-059.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Multiple flaws due to,
- Error when handling process integrity level assignments and EUC-JP character encoding.
- Multiple unspecified errors.
Impact:
Successful exploitation will allow attackers to corrupt memory by the execution of arbitrary code in the context of the current user.
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://technet.microsoft.com/en-us/security/bulletin/ms13-059
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (c) 2013 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 11 $

Serious:

Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (2870699)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903320
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS13-069.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Multiple unspecified errors.
Impact:
Successful exploitation will allow attackers to corrupt memory by the execution of arbitrary code in the context of the current user.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://technet.microsoft.com/en-us/security/bulletin/ms13-069
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 11 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2888505)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903329
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS13-088.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Multiple flaws are due to,
- An error when generating print previews of certain web content.
- An error when handling CSS special characters.
- An use-after-free error when handling CAnchorElement objects.
- Multiple unspecified errors.
Impact:
Successful exploitation will allow attackers to corrupt memory by the execution of arbitrary code, disclose potentially sensitive information and compromise a user's system.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x
Microsoft Internet Explorer version 11.x on Windows 8.1 x32/x64 and Windows server 2012 R2.
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-088
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 64 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2898785)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903330
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS13-097.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Multiple flaws are due to,
- An unspecified error exists during validation of local file installation.
- An unspecified error exists during secure creation of registry keys.
- Multiple unspecified errors.
Impact:
Successful exploitation will allow attackers to corrupt memory by the execution of arbitrary code, bypass certain security restrictions and compromise a user's system.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://technet.microsoft.com/en-us/security/bulletin/ms13-097
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 114 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2909921)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903336
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS14-010.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Multiple flaws are due to,
- An unspecified error exists during validation of local file installation and secure creation of registry keys.
- An error within the VBScript engine.
- Multiple unspecified errors.
Impact:
Successful exploitation will allow attackers to corrupt memory by the execution of arbitrary code, bypass certain security restrictions and compromise a user's system.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-010
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 263 $

Serious:

Microsoft .NET Framework Multiple Vulnerabilities (2916607)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903337
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS14-009.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Multiple flaws due to,
- ASP.NET does not properly identify stale HTTP connections.
- An error within the .NET framework when handling certain COM objects.
- Additionally, some unspecified weakness exists.
Impact:
Successful exploitation could allow an attacker to bypass certain security
mechanism and cause denial of service.
Affected Software/OS:
Microsoft .NET Framework 1.0, 1.1, 2.0, 3.0, 3.5, 3.5.1, 4.0, 4.5 and 4.5.1
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms14-009
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 SecPod
Summary: Check for the version of vulnerable files
Version: $Revision: 263 $

Serious:

Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (2761226)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902693
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-075.
Vulnerability Insight:
Multiple flaws are due to
- Use-after-free error within win32k.sys when handling objects in memory.
- An error when parsing a specially crafted 'TrueType' font file.
Impact:
Successful exploitation will allow remote attackers to execute arbitrary
code with kernel-mode privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-075
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 12 $

Serious:

Microsoft .NET Framework Remote Code Execution Vulnerabilities (2878890)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903412
Summary:
This host is missing an critical security update according to
Microsoft Bulletin MS13-082.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Multiple flaws are due to,
- An unspecified error when handling OpenType fonts (OTF).
- An error when when expanding entity references.
- An unspecified error when parsing JSON data.
Impact:
Successful exploitation will allow remote attackers to execute the arbitrary
code, exhaust available system resource, cause a DoS (Denial of Service)
and compromise the system.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework 2.x
Microsoft .NET Framework 3.x
Microsoft .NET Framework 4.x
Solution:
Run Windows Update and update the listed hotfixes or download and update
mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-082
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable version of files
Version: $Revision: 11 $

Serious:

MS Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (2870008)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903500
Summary:
This host is missing an critical security update according to
Microsoft Bulletin MS13-081
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Multiple flaws are due to ,
- An error when parsing OpenType fonts (OTF) can be exploited to corrupt memory.
- An error when handling the USB descriptor of inserted USB devices can be exploited to corrupt memory.
- A use-after-free error within the kernel-mode driver (win32k.sys) can be exploited to gain escalated privileges.
- An error when handling objects in memory related to App Containers can be exploited to disclose information from a different App Container.
- An error related to NULL page handling within the kernel-mode driver (win32k.sys) can be exploited to gain escalated privileges.
- A double fetch error within the DirectX graphics kernel subsystem (dxgkrnl.sys) can be exploited to gain escalated privileges.
- An error when parsing the CMAP table while rendering TrueType fonts (TTF) can be exploited to corrupt memory.
Impact:
Successful exploitation will allow remote attackers to execute arbitrary
code with kernel-mode privileges and take complete control of the affected
system.
Impact Level: System
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update
mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-081
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable files version
Version: $Revision: 496 $

Serious:

MS Windows Scripting Runtime Object Library RCE Vulnerability (2909158)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903505
Summary:
This host is missing an critical security update according to Microsoft Bulletin MS13-099.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
The flaw is due to memory corruption resulting from improperly handling of an object in memory by Scripting Runtime Object Library.
Impact:
Successful exploitation will allow attackers to execute arbitrary code, cause a DoS (Denial of Service), and compromise the vulnerable system.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
Microsoft Windows 8 x32/x64
Microsoft Windows 8.1 x32/x64
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms13-099
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Scrrun.dll' file version
Version: $Revision: 116 $

Serious:

MS Windows Kerberos Checksum Remote Privilege Escalation Vulnerability (3011780)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804799
NODESC
CVSS Base Score : 9.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 823 $

Serious:

Microsoft Windows Print Spooler Components Privilege Escalation Vulnerability (2839894)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903212
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-050.
Vulnerability Insight:
The vulnerability is caused due to improper memory operations performed by
the affected software when deleting printer connections.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code with system privileges, resulting in complete compromise of the target.
Impact Level: System
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-050
CVSS Base Score : 9.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Win32spl.dll' file version
Version: $Revision: 11 $

Serious:

Microsoft Group Policy Remote Code Execution Vulnerability (3000483)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:805448
NODESC
CVSS Base Score : 8.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1015 $

Serious:

Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (2783534)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902936
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-078.
Vulnerability Insight:
- An error in the OpenType Font (OTF) driver when handling certain objects
can be exploited via a specially crafted font file.
- An error when handling certain TrueType Fonts (TTF) can be exploited
via a specially crafted font file.
Impact:
Successful exploitation will allow remote attackers to execute arbitrary
code with kernel-mode privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-078
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable files version
Version: $Revision: 12 $

Serious:

Microsoft .NET Framework Privilege Elevation Vulnerability (2800277)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902950
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-015.
Vulnerability Insight:
The flaw is due to an error when handling permissions of a callback function
when a certain WinForm object is created and can be exploited to bypass CAS
(Code Access Security) restrictions via a specially crafted XAML Browser
Application (XBAP) or an untrusted .NET application.
Impact:
Successful exploitation could allow an attacker to execute arbitrary code.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework 4
Microsoft .NET Framework 4.5
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 2.0 Service Pack 2
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-015
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the version of 'system.windows.forms.dll' file
Version: $Revision: 11 $

Serious:

Microsoft Windows Networking Components Remote Code Execution Vulnerabilities (2733594)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903036
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-054.
Vulnerability Insight:
The flaws are due to
- The way windows networking components handle a specially crafted RAP
response.
- A format string error within the print spooler service can be exploited
via a specially crafted response.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code on an affected system or cause denial of service condition.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-054
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Netapi32.dll' and 'Localspl.dll' file version
Version: $Revision: 12 $

Serious:

Microsoft Comctl32 Integer Overflow Vulnerability (2864058)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903225
Summary:
This host is missing an critical security update according to Microsoft Bulletin MS13-083.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
A flaw exist in Comctl32.dll file which is caused by an integer overflow in the common control library.
Impact:
Successful exploitation will allow attackers to execute arbitrary code on the system with elevated privileges.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2003 x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 R2 for x64 Service Pack 1 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://technet.microsoft.com/en-us/security/bulletin/ms13-083
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (c) 2013 SecPod
Summary: Check for the vulnerable 'Comctl32.dll' file version
Version: $Revision: 11 $

Serious:

Microsoft Windows NAT Driver Denial of Service Vulnerability (2849568)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903317
Summary:
This host is missing an important security update according to Microsoft Bulletin MS13-062.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Flaw is due to an improper handling asynchronous RPC requests.
Impact:
Successful exploitation will allow attackers to execute arbitrary code and take complete control of an affected system.
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://technet.microsoft.com/en-us/security/bulletin/ms13-062
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Rpcrt4.dll' file version
Version: $Revision: 11 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2977629)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:802081
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 787 $

Serious:

Microsoft SMB Transaction Parsing Remote Code Execution Vulnerability
Risk:Serious
Application:microsoft-ds
Port:445
Protocol:tcp
ScriptID:902660
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-020.
Vulnerability Insight:
The flaw is due to improper validation of field in SMB request,
which allows remote attackers to execute arbitrary code on the system by
sending a malformed SMB request.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code on the system.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 SP1 and prior
Microsoft Windows 2008 SP2 and prior
Microsoft Windows Vista SP2 and prior
Microsoft Windows 2008 R2 SP1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2003 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/MS11-020
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: attack
Copyright: Copyright (C) 2012 SecPod
Summary: Determine if SMB server is prone to remote code execution vulnerability
Version: $Revision: 1039 $

Serious:

Microsoft Windows IME (Japanese) Privilege Elevation Vulnerability (2992719)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:802088
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 818 $

Serious:

Microsoft Unauthorized Digital Certificates Spoofing Vulnerability (2728973)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:802912
Summary:
This host is installed with Microsoft Windows operating system and
is prone to Spoofing vulnerability.
Vulnerability Insight:
Microsoft certificate authorities, which are stored outside the recommended
secure storage practices can be misused. An attacker could use these
certificates to spoof content, perform phishing attacks, or perform
man-in-the-middle attacks.
Impact:
Successful exploitation could allow remote attackers to use the
certificates to spoof content, perform phishing attacks, or perform
man-in-the-middle attacks.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Apply the Patch from below link,
http://support.microsoft.com/kb/2728973
CVSS Base Score : 9.3
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH
Summary: Check if affected certificates are Untrusted Certificates
Version: $Revision: 12 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2969262)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804595
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS14-035.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Multiple flaws are due to,
- A use-after-free error when handling CMarkup objects.
- An error when handling negotiation of certificates during a TLS session.
- Improper validation of certain permissions.
- and multiple Unspecified errors.
Impact:
Successful exploitation will allow attackers to conduct session hijacking attacks, disclose potentially sensitive information, bypass certain security restrictions, and compromise a user's system.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-035
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 758 $

Serious:

Microsoft Internet Explorer Remote Code Execution Vulnerability (2757760)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:803028
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-063.
Vulnerability Insight:
Multiple vulnerabilities exists due to the way that Internet Explorer
accesses an object that has been deleted and causing multiple
use-after-free errors when,
- Handling onMove events, event listeners aand the execCommand method.
- Cloning nodes and layout handling.
Impact:
Successful exploitation could allow remote attackers to gain sensitive
information or execute arbitrary code in the context of the current user.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-063
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (c) 2012 Greenbone Networks GmbH
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 12 $

Serious:

MS Internet Explorer Remote Code Execution Vulnerability (2847140)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:803395
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS13-038.
Vulnerability Insight:
use-after-free error when handling 'CGenericElement'
Impact:
Successful exploitation will allow remote attackers to execute arbitrary code
and failed attacks will cause denial of service conditions.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 8.x and 9.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-038
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 11 $

Serious:

Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (2879017)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804004
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS13-080.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Multiple flaws are due to,
- Use-after-free error within mshtml.dll when handling certain objects.
- Use-after-free error when handling the 'onpropertychange' event in CDisplayPointer.
- Multiple unspecified errors.
Impact:
Successful exploitation will allow attackers to corrupt memory by the execution of arbitrary code in the context of the current user.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x
Microsoft Internet Explorer version 11.x on Windows 8.1
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-080
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (c) 2013 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 11 $

Serious:

Microsoft ASP.NET Insecure Site Configuration Vulnerability (2905247)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804038
Summary:
This host is missing an important security update according to Microsoft advisory (2905247).
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Flaw is due to the view state that exists when Machine Authentication Code (MAC) validation is disabled through configuration settings.
Impact:
Successful exploitation will allow remote attackers to use specially crafted HTTP content to inject code to be run in the context of the service account on the ASP.NET server.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework versions 1.1, 2.0, 3.5, 3.5.1, 4.0, 4.5 and 4.5.1
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/advisory/2905247
CVSS Base Score : 9.3
Family name: Windows
Category: infos

Summary: Check for the vulnerable 'aspnet_wp.exe' file version
Version: $Revision: 143 $

Serious:

Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (2925418)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804500
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS14-012.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Multiple flaws are due to, error when handling CMarkup objects and multiple unspecified errors.
Impact:
Successful exploitation will allow attackers to execute arbitrary code, corrupt memory and compromise a user's system.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-012
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 323 $

Serious:

Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (2950467)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804535
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS14-018.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Multiple unspecified error when handling objects in memory.
Impact:
Successful exploitation will allow attackers to execute arbitrary code, corrupt memory and compromise a user's system.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/11.x
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-018
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 758 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2962482)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804579
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS14-029.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Multiple unspecified flaws are due to user-supplied input is not properly sanitized.
Impact:
Successful exploitation will allow attackers to corrupt memory by the execution of arbitrary code in the context of the current user.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-029
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 758 $

Serious:

Microsoft Windows Graphics Component Multiple Vulnerabilities (2967487)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804596
Summary:
This host is missing a critical security update according to Microsoft
Bulletin MS14-036.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Multiple flaws are due to,
- An error within Unicode Scripts Processor.
- An error within GDI+ when validating images.
Impact:
Successful exploitation will allow attackers to execute arbitrary code
and compromise a user's system.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 8 x32/x64
Microsoft Windows 8.1 x32/x64
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Microsoft Windows 2003 x32 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms14-036
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable file version
Version: $Revision: 496 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2976627)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804739
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS14-051.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Flaws are due to multiple unspecified errors.
Impact:
Successful exploitation will allow attackers to execution of arbitrary code and compromise a user's system.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-051
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 758 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2987107)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804776
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 787 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2975687)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804713
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS14-037.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Multiple flaws are due to,
- An error when handling EV (Extended Validation) SSL certificates.
- and multiple Unspecified errors.
Impact:
Successful exploitation will allow attackers to bypass certain security restrictions and compromise a user's system.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms14-037
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 758 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (3003057)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804790
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1032 $

Serious:

Microsoft .NET Framework Privilege Elevation Vulnerability (3005210)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804791
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 818 $

Serious:

MS Windows Kernel-Mode Driver Privilege Escalation and RCE Vulnerabilities (3000061)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804859
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 787 $

Serious:

Windows OLE Object Handling Arbitrary Code Execution Vulnerability (3000869)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804860
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 787 $

Serious:

MS Windows XML Core Services Remote Code Execution Vulnerability (2993958)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804879
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 818 $

Serious:

Microsoft Windows OLE Object Handling Code Execution Vulnerabilities (3011443)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:805015
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 803 $

Serious:

Microsoft Adobe Font Driver Remote Code Execution Vulnerabilities (3032323)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:805052
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1076 $

Serious:

Microsoft Windows Remote Code Execution Vulnerabilities (3041836)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:805053
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1076 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (3008923)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:805112
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 863 $

Serious:

Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (3034682)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:805136
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1005 $

Serious:

Microsoft .NET Framework Remote Code Execution Vulnerability (3000414)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804777
NODESC
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 787 $

Serious:

Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (3032359)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:805143
NODESC
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1076 $

Serious:

Microsoft Media Decompression Remote Code Execution Vulnerability (979902)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:900246
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS10-033.
Vulnerability Insight:
An unspecified error exists while processing media files with a specially
crafted compression data. An attacker can exploit this vulnerability by
tricking a user to open a specially crafted media file.
Impact:
Successful exploitation will allow remote attackers to execute arbitrary
code.
Impact Level: System
Affected Software/OS:
DirectX, Windows Media Encoder 9 and COM component on,
Micorsoft Windows 7
Microsoft Windows 2000 SP4
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 1/2 and prior.
Microsoft Windows Server 2008 Service Pack 1/2 and prior.
Windows Media Format Runtime 9 on,
Microsoft Windows 2000 SP4
Microsoft Windows XP Service Pack 3 and prior
Windows Media Format Runtime 9.5 on,
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Windows Media Format Runtime 11 on,
Microsoft Windows XP Service Pack 3 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms10-033.mspx
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the version of Directx, Media Format Runtime, Media Encoder and Hotfix
Version: $Revision: 14 $

Serious:

Microsoft Remote Desktop Client Remote Code Execution Vulnerability (2508062)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:900273
Summary:
This host is missing a critical security update according to Microsoft
Bulletin MS11-017.
Vulnerability Insight:
The flaw is caused by the way Windows Remote Desktop Client handles loading
of DLL files. Remote attacker can execute arbitrary code by tricking a user
to open a legitimate Remote Desktop configuration file (.rdp) that
is located in the same network directory as a specially crafted dynamic
link library (DLL) file.
Impact:
Successful exploitation could allow authenticated attackers to execute
arbitrary code with elevated privileges.
Impact Level: System
Affected Software/OS:
Remote Desktop Connection 5.2 Client
- Windows XP Service Pack 3 and prior
Remote Desktop Connection 6.0/6.1 Client
- Windows XP Service Pack 3
- Windows Vista Service Pack 2 and prior
- Windows Server 2003 Service Pack 2 and prior
- Windows Server 2008 Service Pack 2 and prior
Remote Desktop Connection 7.0 Client
- Windows 7
- Windows XP Service Pack 3 and prior
- Windows Vista Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/Bulletin/MS11-017.mspx
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Mstscax.dll' file version
Version: $Revision: 13 $

Serious:

Microsoft IE Developer Tools WMITools and Windows Messenger ActiveX Control Vulnerability (2508272)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:900281
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-027.
Vulnerability Insight:
An unspecified error exists in the IE Developer Tools(iedvtool.dll), WMITools
(WBEMSingleView.OCX) and Windows Messenger (msgsc.dll) ActiveX Controls when
used with Internet Explorer. Attackers can execute arbitrary code by tricking
a user into visiting a specially crafted web page.
Impact:
Successful exploitation will allow remote attackers to execute arbitrary
code.
Impact Level: System.
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 1/2 and prior
Microsoft Windows Server 2008 Service Pack 1/2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/Bulletin/MS11-027.mspx
Workaround:
Set the killbit for the following CLSIDs,
{1a6fe369-f28c-4ad9-a3e6-2bcb50807cf1}, {2745E5F5-D234-11D0-847A-00C04FD7BB08}
{FB7199AB-79BF-11d2-8D94-0000F875C541}
http://support.microsoft.com/kb/240797
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the CLSID and Hotfix
Version: $Revision: 346 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2482017)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:901180
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-003.
Vulnerability Insight:
Multiple flaws are caused by memory corruptions, uninitialized memory and
insecure library loading errors when processing certain HTML or JavaScript
data, which could be exploited by attackers to execute arbitrary code by
tricking a user into visiting a malicious web page.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code in the context of the application. Failed exploit attempts will result
in denial-of-service conditions.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/Bulletin/MS11-003.mspx
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'lepeers.dll' file version
Version: $Revision: 13 $

Serious:

Microsoft Windows Components Remote Code Execution Vulnerabilities (2570947)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:901205
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-071.
Vulnerability Insight:
The flaw exists when specific Windows components incorrectly restrict the
path used for loading external libraries. An attacker can exploit this
issue by enticing an unsuspecting victim to open a file on a remote SMB
or WebDAV share.
Impact:
Successful exploitation could allow remote attacker to execute arbitrary
code by enticing an unsuspecting victim to open a file on a remote SMB or
WebDAV share.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior.
Microsoft Windows XP Service Pack 3 and prior.
Microsoft Windows 2003 Service Pack 2 and prior.
Microsoft Windows Vista Service Pack 2 and prior.
Microsoft Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-071
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the registry and vulnerable file version
Version: $Revision: 13 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2586448)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:901208
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-081.
Vulnerability Insight:
Multiple flaws are due to the way Internet Explorer handles,
- dereferenced memory address aka 'Select Element'.
- accessing an object that was not properly initialized aka 'Jscript9.dll',
'OLEAuto32.dll'.
- accessing a deleted object aka 'Body Element', 'OnLoad Event',
'Option Element', 'Scroll Event'.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code in the context of the application. Failed exploit attempts will result
in denial-of-service conditions.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-081
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 13 $

Serious:

Microsoft Windows DirectPlay Remote Code Execution Vulnerability (2770660)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:901212
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS12-082.
Vulnerability Insight:
The vulnerability is caused when Windows DirectPlay fails to properly handle
specially crafted office document with embedded content.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code by tricking a user into opening a malicious office document.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-082
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Dpnet.dll' file version
Version: $Revision: 12 $

Serious:

Microsoft Windows Theme File Remote Code Execution Vulnerability (2864063)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:901221
Summary:
This host is missing an important security update according to Microsoft Bulletin MS13-071.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Flaw is caused when Microsoft Windows improperly handles theme and screensaver files.
Impact:
Successful exploitation will allow attackers to execute arbitrary code and take complete control of an affected system.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms13-071
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (c) 2013 SecPod
Summary: Check for the vulnerable 'Themeui.dll' file version
Version: $Revision: 11 $

Serious:

Microsoft Windows ActiveX Control RCE Vulnerability (2900986)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:901225
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS13-090.
Vulnerability Detection:
Get the ActiveX control (CLSID) information from registry and check
appropriate patch is applied or not.
Vulnerability Insight:
Flaw in the InformationCardSigninHelper Class ActiveX control (icardie.dll)
and can be exploited to corrupt the system state.
Impact:
Successful exploitation allows execution of arbitrary code when viewing a
specially crafted web page using Internet Explorer.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows 8.1 x32/x64 Edition
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update
mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-090
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the CLSID and Patch
Version: $Revision: 303 $

Serious:

MS Windows Secure Channel Remote Code Execution Vulnerability (2992611)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:804881
NODESC
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 863 $

Serious:

Microsoft Windows File Handling Component Remote Code Execution Vulnerability (2758857)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:901304
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-081.
Vulnerability Insight:
The flaw is due to error in the File Handling component, which allow user
browses to a folder that contains a file or sub folder names and can be
exploited to corrupt memory via a file with a specially crafted filename.
Impact:
Successful exploitation could allow attacker to gain the same user rights as
the current user by execute arbitrary code with system-level privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms12-081.mspx
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Kernel32.dll' files version
Version: $Revision: 110 $

Serious:

Microsoft Windows Data Access Components Remote Code Execution Vulnerabilities (2451910)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902281
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-002.
Vulnerability Insight:
The flaws are due to:
- A buffer overflow error in the Data Source Name (DSN) argument of an Open
Database Connectivity (ODBC) API that may be used by third-party applications,
which could allow attackers to execute arbitrary code by convincing a user to
visit a specially crafted web page.
- A memory corruption error in the Microsoft Data Access Components (MDAC) when
handling internal data structures, which could be exploited by remote attackers
to execute arbitrary code via a specially crafted web page.
Impact:
Successful exploitation will allow the attacker to execute arbitrary code on
the targeted system.
Impact Level: System/Application
Affected Software/OS:
Micorsoft Windows 7
Microsoft Windows XP Service Pack 3 and prior.
Microsoft Windows 2K3 Service Pack 2 and prior.
Microsoft Windows Vista Service Pack 2 and prior.
Microsoft Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/Bulletin/MS11-002.mspx
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the version of Msadco.dll file
Version: $Revision: 13 $

Serious:

Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902334
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-006.
Vulnerability Insight:
The flaw is due to a signedness error in the 'CreateSizedDIBSECTION()'
function within the Windows Shell graphics processor when parsing thumbnail bitmaps.
Impact:
Successful exploitation will allow attackers to execute arbitrary code by
tricking a user into opening or previewing a malformed Office file or browsing
to a network share, UNC, or WebDAV location containing a specially crafted
thumbnail image.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/Bulletin/MS11-006.mspx
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the version of Shell32.dll file
Version: $Revision: 13 $

Serious:

Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2485376)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902335
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-007.
Vulnerability Insight:
The flaw is caused by an error in the Windows OpenType Compact Font Format
(CFF) driver that does not properly validate the parameter values of
specially crafted OpenType fonts.
Impact:
Successful exploitation will allow the remote attackers or malicious users to
execute arbitrary code with kernel privileges.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior.
Microsoft Windows XP Service Pack 3 and prior.
Microsoft Windows 2K3 Service Pack 2 and prior.
Microsoft Windows Vista Service Pack 2 and prior.
Microsoft Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/Bulletin/MS11-007.mspx
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the version of vulnerable file
Version: $Revision: 13 $

Serious:

Windows OpenType Compact Font Format (CFF) Driver Remote Code Execution Vulnerability (2507618)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902363
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-032.
Vulnerability Insight:
The flaw is caused by a stack overflow error in the OpenType Compact Font
Format (CFF) driver when handling parameter values of OpenType fonts.
Impact:
Successful exploitation will allow remote attackers execute arbitrary code
via a malicious OpenType font, or by local attackers to gain elevated
privileges.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/Bulletin/MS11-032.mspx
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the version of vulnerable Atmfd.dll file
Version: $Revision: 13 $

Serious:

Microsoft Windows OLE Automation Remote Code Execution Vulnerability (2476490)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902377
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-038.
Vulnerability Insight:
The flaw is due to an error in Object Linking and Embedding (OLE)
Automation (oleaut32.dll) when parsing a Windows Metafile (WMF) images.
Impact:
Successful exploitation could allow attackers to execute arbitrary code in the
context of the user running the application, which can compromise the
application and possibly the computer.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/MS11-038.mspx
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Oleaut32.dll' file version
Version: $Revision: 13 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2530548)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902443
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-050.
Vulnerability Insight:
Multiple flaws are due to, the way Internet Explorer enforces the content
settings supplied by the Web server, handles HTML sanitization using
toStaticHTML, handles objects in memory, and handles script during certain
processes.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code in the context of the application. Failed exploit attempts will result
in denial-of-service conditions.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/Bulletin/MS11-050.mspx
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 13 $

Serious:

Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (2567053)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902483
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-077.
Vulnerability Insight:
Multiple flaws are due to,
- A privilege elevation vulnerability exists in the way that kernel-mode
drivers validate data supplied from user mode to kernel mode.
- A denial of service vulnerability exists in implementations of windows
when the system improperly processes a specially crafted TrueType font
file.
- An remote code execution vulnerability exists in the Windows kernel due
to improper handling of a specially crafted font (.fon) file.
- A privilege elevation vulnerability exists due to the way that Windows
Kernel-mode drivers manage kernel-mode driver objects.
Impact:
Successful exploitation could allow local attackers to gain elevated
privileges or to run arbitrary code in kernel mode and take complete control
of an affected system. An attacker could then install programs view, change,
or delete data or create new accounts with full administrative rights.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2003 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-077
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 13 $

Serious:

Windows Mail and Windows Meeting Space Remote Code Execution Vulnerability (2620704)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902486
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-085.
Vulnerability Insight:
The flaw is due to Windows Mail and Windows Meeting Space loading
certain libraries in an insecure manner. This can be exploited to load
arbitrary libraries by tricking a user into opening an EML or WCINV file
located on a remote WebDAV or SMB share.
Impact:
Successful exploitation could allow remote attacker to execute the arbitrary
code or compromise a user's system.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-085.mspx
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'wab32.dll' file version
Version: $Revision: 13 $

Serious:

Microsoft JScript and VBScript Scripting Engines Remote Code Execution Vulnerability (2514666)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902501
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-031.
Vulnerability Insight:
The flaw is caused by an integer overflow error in the JScript and VBScript
scripting engines when reallocating memory while decoding a script in order
to run it, which could be exploited by remote attackers to execute arbitrary
code via a malicious web page.
Impact:
Successful exploitation could allow remote attackers to crash an affected
system or execute arbitrary code by tricking a user into visiting a specially
crafted web page.
Impact Level: System/Application
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-031.mspx
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the version of 'Vbscript.dll' file
Version: $Revision: 13 $

Serious:

Microsoft SMB Client Remote Code Execution Vulnerabilities (2511455)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:900279
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-019.
Vulnerability Insight:
The flaws are due to,
- errors in SMB client implementation which fails to validate specially
crafted SMB responses.
- error in CIFS Browser Protocol implementation which fails to parse
specially crafted Computer Browser messages causing memory corruption.
Impact:
Successful exploitation could allow remote attacker to execute arbitrary
code by creating a specially crafted browser message and sending the message
to an affected system or attacker could perform a man-in-the-middle attack
to respond to a legitimate SMB request with a malformed SMB response.
Impact Level: System
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2003 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 1/2 and prior
Microsoft Windows Server 2008 Service Pack 1/2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/Bulletin/MS11-019.mspx
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Mrxsmb.sys' file version
Version: $Revision: 13 $

Serious:

Microsoft .NET Framework Remote Code Execution Vulnerability (2484015)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902502
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-028.
Vulnerability Insight:
The flaw is caused by a stack corruption error in the x86 JIT compiler within
the .NET Framework when compiling certain types of function calls, which
could be exploited by remote attackers to execute arbitrary code by tricking
a user into visiting a specially crafted web page.
Impact:
Successful exploitation could allow remote attackers to crash an affected
system or execute arbitrary code by tricking a user into visiting a specially
crafted web page.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework 4.0
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.5 Service Pack 1
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-028
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the version of 'mscorlib.dll' file
Version: $Revision: 13 $

Serious:

Microsoft .NET Framework and Silverlight Remote Code Execution Vulnerability (2514842)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902523
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-039.
Vulnerability Insight:
The flaw is due to an input validation error when passing values to
trusted APIs. This can be exploited to access memory in an unsafe manner via
a specially crafted XAML Browser Application or Silverlight application.
Impact:
Successful exploitation could allow attacker to execute arbitrary code within
the context of the application.
Impact Level: System/Application
Affected Software/OS:
Microsoft Silverlight 4.0
Microsoft .NET Framework 4.0
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 3.5 Service Pack 1
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 2.0 Service Pack 1
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-039
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the version of 'System.dll' file
Version: $Revision: 13 $

Serious:

Microsoft .NET Framework and Silverlight Remote Code Execution Vulnerability (2604930)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902581
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-078.
Vulnerability Insight:
The flaw due to an error when restricting inheritance within classes
and can be exploited via a specially crafted web page.
Impact:
Successful exploitation could allow attacker to execute arbitrary code within
the context of the affected application. Failed exploit attempts will likely
result in a denial-of-service condition.
Impact Level: System/Application
Affected Software/OS:
Microsoft Silverlight 4.0
Microsoft .NET Framework 4.0
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 1.1 Service Pack 1
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-078
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the version of 'mscorlib.dll' file
Version: $Revision: 13 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2559049)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902613
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-057.
Vulnerability Insight:
Multiple flaws are due to, the way Internet Explorer handles objects in
memory, handles JavaScript event handlers, accesses files stored in the
local machine, renders data during certain processes and the way the telnet
handler executes the associated application.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code in the context of the application. Failed exploit attempts will result
in denial-of-service conditions.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-057.mspx
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 13 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2618444)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902642
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-099.
Vulnerability Insight:
Multiple flaws are due to the way Internet Explorer handles,
- the XSS filter,
- loading of external libraries ie .DLL files and
- the content settings supplied by the Web server.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code in the context of the application. Failed exploit attempts will result
in denial-of-service conditions.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-099
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 13 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2647516)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902649
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-010.
Vulnerability Insight:
Multiple flaws are due to the way Internet Explorer handles,
- the content during copy and paste processes,
- the objects in memory that has been deleted,
- the NULL bytes during creation and initialization of strings.
Impact:
Successful exploitation could allow remote attackers to gain sensitive
information or execute arbitrary code in the context of the application.
Failed exploit attempts will result in denial-of-service conditions.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-010
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 12 $

Serious:

MS Windows C Run-Time Library Remote Code Execution Vulnerability (2654428)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902653
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-013.
Vulnerability Insight:
The flaw is due to the way 'Msvcrt.dll' calculates the size of a
buffer in memory, allowing data to be copied into memory that has not been
properly allocated.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code as the logged-on user.
Impact Level: System
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior.
Microsoft Windows Vista Service Pack 2 and prior.
Microsoft Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-013
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Msvcrt.dll' file version
Version: $Revision: 12 $

Serious:

Windows ClickOnce Application Installer Remote Code Execution Vulnerability (2584146)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902657
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS12-005.
Vulnerability Insight:
The flaw is due to an error within the Windows Packager when
loading ClickOnce applications embedded in Microsoft Office files.
Impact:
Successful exploitation could allow local attackers to run arbitrary code
and take complete control of an affected system. An attacker can gain
administrative rights.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior.
Microsoft Windows XP Service Pack 3 and prior.
Microsoft Windows 2003 Service Pack 2 and prior.
Microsoft Windows Vista Service Pack 2 and prior.
Microsoft Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-005
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Packager.exe/Packager.dll' file version
Version: $Revision: 12 $

Serious:

Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902663
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-020.
Vulnerability Insight:
The flaws are due to the way Remote Desktop Protocol accesses an
object in memory that has been improperly initialized or has been deleted
and the way RDP service processes the packets.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code as the logged-on user or cause a denial of service condition.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-020
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable file version
Version: $Revision: 12 $

Serious:

Windows Authenticode Signature Remote Code Execution Vulnerability (2653956)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902669
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-024.
Vulnerability Insight:
The flaw is due to the way Windows Authenticode Signature Verification
function verifies portable executable (PE) files, which can be exploited to
add malicious code to the file without invalidating the signature.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code as the logged-on user.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2003 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-024
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Wintrust.dll' file version
Version: $Revision: 12 $

Serious:

Microsoft Windows SMB Server Remote Code Execution Vulnerability (2508429)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:900280
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-020.
Vulnerability Insight:
The flaw is caused when Microsoft Server Message Block (SMB) protocol
software improperly handles SMB packets, including some pre-authentication
scenarios.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary code
and cause a denial of service or compromise a vulnerable system.
Impact Level: System
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 1/2 and prior
Microsoft Windows Server 2008 Service Pack 1/2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/Bulletin/MS11-020.mspx
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the version of Srv.sys file
Version: $Revision: 13 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2675157)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902670
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-023.
Vulnerability Insight:
Multiple flaws are due to an,
- Unspecified error in the Print feature.
- Error in the handling of the onReadyStateChange event, VML styles
and JScript9 when accessing already deleted.
Impact:
Successful exploitation could allow remote attackers to gain sensitive
information or execute arbitrary code in the context of the application.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-023
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 12 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2699988)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902682
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-037.
Vulnerability Insight:
Multiple vulnerabilities are due to the way that Internet Explorer,
- Handles content using specific strings when sanitizing HTML.
- Handles EUC-JP character encoding.
- Processes NULL bytes, which allows to disclose content from the process memory.
- Accesses an object that has been deleted, which allows to corrupt memory using Internet Explorer Developer Toolbar.
- Accesses an object that does not exist, when handling the 'Col' element.
- Accesses an object that has been deleted, when handling Same ID Property, 'Title' element, 'OnBeforeDeactivate' event, 'insertRow' method and 'OnRowsInserted' event allows to corrupt memory.
- Accesses an undefined memory location, when handling the 'insertAdjacentText' method allows to corrupt memory.
- Handles 'Scrolling' event.
Impact:
Successful exploitation could allow remote attackers to gain sensitive information or execute arbitrary code in the context of the application.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-037
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 12 $

Serious:

Microsoft Remote Desktop Protocol Remote Code Execution Vulnerability (2685939)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902683
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-036.
Vulnerability Insight:
The way that the Remote Desktop Protocol accesses an object in memory that
has been improperly initialized or has been deleted or the way RDP service
processes the packets, allows to run arbitrary code on the target system.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code as the logged-on user or cause a denial of service condition.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-036
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Rdpwd.sys' file version
Version: $Revision: 12 $

Serious:

Microsoft Windows Data Access Components Remote Code Execution Vulnerability (2698365)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902687
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-045.
Vulnerability Insight:
Vulnerability is due to the way that Microsoft Data Access Components
accesses an object in memory that has been improperly initialized when
parsing XML code.
Impact:
Successful exploitation could allow remote attackers to gain sensitive
information or execute arbitrary code in the context of the current user.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-045
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Msado15.dll' file version
Version: $Revision: 12 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2761465)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902696
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-077.
Vulnerability Insight:
Multiple vulnerabilities are due to use-after-free errors within the
'InjectHTMLStream()' function, 'CMarkup' class and 'Ref Counting'.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code in the context of the user.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-077
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 110 $

Serious:

Microsoft Internet Explorer Remote Code Execution Vulnerability (2794220)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902699
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS13-008.
Vulnerability Insight:
Flaw exists due to the way that Internet Explorer accesses an object that has
been deleted or has not been properly allocated and causing use-after-free
error when handling the CDwnBindInfo object.
Impact:
Successful exploitation could will remote attackers to gain sensitive
information or execute arbitrary code in the context of the current user.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-008
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (c) 2013 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 11 $

Serious:

Microsoft Active Accessibility Remote Code Execution Vulnerability (2623699)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902746
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-075.
Vulnerability Insight:
The flaw is due to a way that the Microsoft Active Accessibility
component handles the loading of DLL files. This can be exploited to load
arbitrary libraries by tricking a user into opening a file located on a
remote WebDAV or SMB share.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code in the context of the user running the vulnerable application.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-075
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Oleacc.dll' file version
Version: $Revision: 13 $

Serious:

Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (2567053)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902767
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-087.
Vulnerability Insight:
The flaw is due to to an error within the Win32k kernel-mode driver
(win32k.sys) when parsing TrueType fonts.
Impact:
Successful exploitation could allow local attackers to run arbitrary code in
kernel mode and take complete control of an affected system. An attacker
could then install programs view, change, or delete data or create new
accounts with full administrative rights.
Impact Level: System
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2003 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-087
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 13 $

Serious:

Microsoft Windows Kernel Security Feature Bypass Vulnerability (2644615)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902783
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS12-001.
Vulnerability Insight:
The flaw is due to an error in the way the kernel (ntdll.dll) loads
structured exception handling tables and allows bypassing the SafeSEH
security mechanism. This facilitates easier exploitation of other
vulnerabilities in affected applications to execute code.
Impact:
Successful exploitation could allow attackers to execute arbitrary code by
leveraging memory corruption vulnerabilities in Windows applications.
Impact Level: System
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior.
Microsoft Windows 2003 Service Pack 2 and prior.
Microsoft Windows Vista Service Pack 2 and prior.
Microsoft Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-001
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Ntdll.dll' file version
Version: $Revision: 12 $

Serious:

MS Windows Color Control Panel Remote Code Execution Vulnerability (2643719)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902791
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS12-012.
Vulnerability Insight:
The flaw is due to a Color Control Panel library used by the Color
Control Panel application is loading libraries in an insecure manner.
Impact:
Successful exploitation allows an attackers to use the vulnerable application
to open a file from a network share location that contains a specially
crafted Dynamic Link Library (DLL) file.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-012
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Colorcpl.exe' file version
Version: $Revision: 12 $

Serious:

Microsoft SMB Client Remote Code Execution Vulnerabilities (2536276)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:900287
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-043.
Vulnerability Insight:
The flaws are due to errors in SMB client implementation which fails to
validate specially crafted SMB responses.
Impact:
Successful exploitation could allow remote attacker to execute arbitrary code
by creating a specially crafted SMB responses.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2003 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 1/2 and prior
Microsoft Windows Server 2008 Service Pack 1/2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/MS11-043.mspx
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Mrxsmb.sys' file version
Version: $Revision: 13 $

Serious:

Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902806
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-100.
Vulnerability Insight:
- An error within ASP.NET when hashing form posts and updating a hash table.
This can be exploited to cause a hash collision resulting in high CPU
consumption via a specially crafted form sent in a HTTP POST request.
- Open redirect vulnerability in the Forms Authentication feature in the
ASP.NET subsystem allows remote attackers to redirect users to arbitrary
web sites and conduct phishing attacks via a crafted return URL.
- The Forms Authentication feature in the ASP.NET subsystem allows remote
authenticated users to obtain access to arbitrary user accounts via a
crafted username.
- The Forms Authentication feature in the ASP.NET subsystem when sliding
expiry is enabled, does not properly handle cached content, which allows
remote attackers to obtain access to arbitrary user accounts via a crafted
URL.
Impact:
Successful exploitation could allow attacker to cause a denial of service,
conduct spoofing attacks or bypass certain security restrictions.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework 4
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 3.5 Service Pack 1
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 1.1 Service Pack 1
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-100
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the version of different files
Version: $Revision: 13 $

Serious:

Microsoft Windows Media Could Allow Remote Code Execution Vulnerabilities (2636391)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902807
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-004.
Vulnerability Insight:
- An unspecified error in the Windows multimedia library (winmm.dll) when
parsing MIDI files can be exploited via a specially crafted file opened
in Windows Media Player.
- An unspecified error exists in the Line21 DirectShow filter (Quartz.dll
and Qdvd.dll) when parsing specially crafted media files.
Impact:
Successful exploitation will allow the attacker to execute arbitrary code in
the context of the user running the application which can compromise the
application and possibly the computer.
Impact Level: System/Application
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior.
Microsoft Windows XP Service Pack 3 and prior.
Microsoft Windows 2003 Service Pack 2 and prior.
Microsoft Windows Vista Service Pack 2 and prior.
Microsoft Windows Server 2008 Service Pack 2 and prior.
Microsoft Windows Media Center TV Pack for Windows Vista.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-004
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable file versions
Version: $Revision: 12 $

Serious:

Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (2660465)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902810
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-008.
Vulnerability Insight:
Multiple flaws are due to
- An error in win32k.sys when validating input passed from user mode through
the kernel component of GDI can be exploited to corrupt memory via a
specially crafted web page containing an IFRAME with an overly large
'height' attribute viewed using the Apple Safari browser.
- A use-after-free error in win32k.sys when handling certain keyboard layouts
can be exploited to dereference already freed memory and gain escalated
privileges.
Impact:
Successful exploitation could allow remote attackers to cause a denial of
service and possibly execute arbitrary code with kernel-level privileges.
Impact Level: System
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior.
Microsoft Windows XP Service Pack 3 and prior.
Microsoft Windows 2003 Service Pack 2 and prior.
Microsoft Windows Vista Service Pack 2 and prior.
Microsoft Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-008
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 12 $

Serious:

Microsoft .NET Framework and Microsoft Silverlight Remote Code Execution Vulnerabilities (2651026)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902811
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-016.
Vulnerability Insight:
Multiple flaws are due to
- An unspecified error when handling un-managed objects can be exploited via
a specially crafted XAML Browser Application (XBAP).
- An error when calculating certain buffer lengths can be exploited to corrupt
memory via a specially crafted XAML Browser Application (XBAP).
Impact:
Successful exploitation could allow attacker to execute arbitrary code within
the context of the affected application. Failed exploit attempts will likely
result in a denial-of-service condition.
Impact Level: System/Application
Affected Software/OS:
Microsoft Silverlight 4.0
Microsoft .NET Framework 4.0
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 2.0 Service Pack 2
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-016
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the version of 'System.dll' file
Version: $Revision: 12 $

Serious:

Microsoft .NET Framework Remote Code Execution Vulnerability (2671605)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902828
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-025.
Vulnerability Insight:
The flaw is due to an error within the .NET CRL (Common Language
Runtime) when handling certain parameters passed to a function and can be
exploited via a specially crafted web page.
Impact:
Successful exploitation could allow an attacker to execute arbitrary code
with the privileges of the currently logged-in user. Failed attacks will
cause denial-of-service conditions.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework 4.0
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 1.1 Service Pack 1
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-025
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the version of 'System.Drawing.dll' file
Version: $Revision: 12 $

Serious:

MS Security Update For Microsoft Office, .NET Framework, and Silverlight (2681578)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902832
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-034.
Vulnerability Insight:
Multiple flaws are due to
- An error exists when parsing TrueType fonts.
- An error in the t2embed.dll module when parsing TrueType fonts can be exploited via a specially crafted TTF file.
- An error in GDI+ when handling certain records can be exploited via a specially crafted EMF image file.
- An error in win32k.sys related to certain Windows and Messages handling can be exploited to execute arbitrary code in the context of another process.
- An error in win32k.sys when handling keyboard layout files can be exploited to execute arbitrary code in the context of another process.
- An error in win32k.sys related to scrollbar calculations can be exploited to execute arbitrary code in the context of another process.
Impact:
Successful exploitation could allow an attacker to gain escalated privileges and execute arbitrary code.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework 4
Microsoft Silverlight 4 and 5
Microsoft .NET Framework 3.5.1
Microsoft Office 2003 Service Pack 3
Microsoft Office 2007 Service Pack 2
Microsoft Office 2010 Service Pack 1
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2003 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-034
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the version of vulnerable files
Version: $Revision: 122 $

Serious:

Microsoft .NET Framework Remote Code Execution Vulnerability (2693777)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902833
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-035.
Vulnerability Insight:
The flaws are due to
- An error within the .NET Framework does not properly serialize user input
and can be exploited to treat untrusted input as trusted.
- An error within the .NET Framework does not properly handle exceptions when
serializing objects and can be exploited via partially trusted assemblies.
Impact:
Successful exploitation could allow an attacker to execute arbitrary code
with the privileges of the currently logged-in user. Failed attacks will
cause denial-of-service conditions.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0 SP2, 3.5 SP1, 3.5.1,
and 4
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-035
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the version of vulnerable files
Version: $Revision: 12 $

Serious:

Microsoft .NET Framework Remote Code Execution Vulnerability (2706726)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902841
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-038.
Vulnerability Insight:
The flaw is due to an error within the framework when handling
pointers and can be exploited to corrupt memory via a specially crafted
web page.
Impact:
Successful exploitation could allow an attacker to execute arbitrary code.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework 4
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 2.0 Service Pack 2
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-038
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the version of 'system.windows.forms.dll' file
Version: $Revision: 12 $

Serious:

Microsoft Windows Shell Remote Code Execution Vulnerability (2691442)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902845
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS12-048.
Vulnerability Insight:
The vulnerability is caused when Windows shell does not properly handle
specially crafted file or directory names.
Impact:
Successful exploitation could allow an attacker to execute arbitrary shell
commands with user level privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-048
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Shell32.dll' file version
Version: $Revision: 12 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2722913)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902923
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-052.
Vulnerability Insight:
- An error in the layout handling when accessing an improperly initialized
or deleted object can be exploited to corrupt memory.
- A use-after-free error when asynchronously accessing NULL objects can be
exploited to dereference an already deleted object.
- An error may cause a corrupted virtual function table that has already
been deleted to be accessed.
- An integer overflow error in the JavaScript parsing when calculating the
size of an object in memory during a copy operation can be exploited
to corrupt memory.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code in the context of the of the current user.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-052
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 12 $

Serious:

Microsoft Distributed File System Remote Code Execution Vulnerabilities (2535512)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:900288
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-042.
Vulnerability Insight:
The flaws are due to errors in Microsoft Distributed File System (DFS)
implementation which fails to validates all fields within specially
crafted DFS responses.
Impact:
Successful exploitation could allow remote attacker to execute arbitrary
code by creating a specially crafted DFS responses.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7.
Microsoft Windows XP Service Pack 3 and prior.
Microsoft Windows 2003 Service Pack 2 and prior.
Microsoft Windows Vista Service Pack 1/2 and prior.
Microsoft Windows Server 2008 Service Pack 1/2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/MS11-042.mspx
CVSS Base Score : 10.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable files version
Version: $Revision: 13 $

Serious:

Microsoft .NET Framework Remote Code Execution Vulnerability (2745030)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902934
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS12-074.
Vulnerability Insight:
- An error within permissions checking of objects that perform reflection can
be exploited via a specially crafted XAML Browser Application (XBAP) or an
untrusted .NET application.
- An sanitisation error when processing partially trusted code can be exploited
to disclose certain data via a specially crafted XAML Browser Application
(XBAP) or an untrusted .NET application.
- The Entity Framework component loads certain libraries in an insecure manner,
which can be exploited to load arbitrary libraries by tricking a user into
opening certain files located on a remote WebDAV or SMB share.
- A validation error when acquiring proxy settings via the
Web Proxy Auto-Discovery (WPAD) can be exploited to execute JavaScript code
with reduced restrictions.
- An error within permissions checking of Windows Presentation Foundation (WPF)
objects that perform reflection can be exploited via a specially crafted XAML
Browser Application (XBAP) or an untrusted .NET application.
Impact:
Successful exploitation will allow an attacker to execute arbitrary code
with the privileges of the currently logged-in user. Failed attacks will
cause denial-of-service conditions.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0, 3.5, 3.5.1,
and 4
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-074
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the version of vulnerable files
Version: $Revision: 12 $

Serious:

Microsoft .NET Framework Privilege Elevation Vulnerability (2769324)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902939
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-004.
Vulnerability Insight:
- An error within the System Drawing namespace of Windows Forms when handling pointers can be exploited to bypass CAS (Code Access Security) restrictions and disclose information.
- An error within WinForms when handling certain objects can be exploited to cause a buffer overflow.
- A boundary error within the System.DirectoryServices.Protocols namespace when handling objects can be exploited to cause a buffer overflow.
- A double construction error within the framework does not validate object permissions and can be exploited via a specially crafted XAML Browser Application (XBAP) or an untrusted .NET application.
Impact:
Successful exploitation will allow an attacker to execute arbitrary code
with the privileges of the currently logged-in user. Failed attacks will
cause denial-of-service conditions.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0, 3.5, 3.5.1, 4 and 4.5
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-004
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the version of vulnerable files
Version: $Revision: 11 $

Serious:

Microsoft Windows Media Decompression Remote Code Execution Vulnerability (2780091)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902947
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS13-011.
Vulnerability Insight:
The flaw is due to an error in DirectShow when handling the decompression
of media content, which can be exploited via specially crafted media content.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code with kernel-mode privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-011
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Quartz.dll' file version
Version: $Revision: 11 $

Serious:

MS Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (2850851)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902978
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS13-053.
Vulnerability Insight:
Multiple flaws are due to,
- Unspecified errors within the Windows kernel-mode driver (win32k.sys) when
processing certain objects and can be exploited to cause a crash or execute
arbitrary code with the kernel privilege.
- An error exists within the GDI+ subsystem.
Impact:
Successful exploitation will allow remote attackers to cause a buffer
overflow and execute arbitrary code with kernel privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-053
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 11 $

Serious:

Microsoft Windows DirectWrite Remote Code Execution Vulnerabilities (2848295)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902983
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS13-054.
Vulnerability Insight:
The flaw is due to an error when processing TrueType fonts and can be
exploited to cause a buffer overflow via a specially crafted file.
Impact:
Successful exploitation could allow attackers to execute arbitrary code as
the logged-on use
Impact Level: System
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-054
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Dwrite.dll' file version
Version: $Revision: 11 $

Serious:

Microsoft .NET Framework Multiple Vulnerabilities (2861561)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:902985
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-052.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Multiple flaws due to,
- Improper handling of TrueType font and multidimensional arrays of small
structures
- Improper validation of permissions for certain objects performing reflection
and delegate objects during serialization
Impact:
Successful exploitation could allow an attacker to execute arbitrary code,
bypass security mechanism and take complete control of an affected system.
Affected Software/OS:
Microsoft .NET Framework 1.0, 1.1, 2.0, 3.0, 3.5, 3.5.1, 4.0 and 4.5
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-052
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the version of vulnerable files
Version: $Revision: 11 $

Serious:

Microsoft Windows Graphics Device Interface RCE Vulnerability (2876331)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903226
Summary:
This host is missing a critical security update according to Microsoft
Bulletin MS13-089.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Flaw is due to when Microsoft Windows improperly handles image in a Windows
Write (.wri) document.
Impact:
Successful exploitation will allow attackers to execute arbitrary code or
cause a denial of service condition.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
Microsoft Windows 8 x32/x64
Microsoft Windows 8.1 x32/x64
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-089
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Gdi32.dll' file version
Version: $Revision: 64 $

Serious:

Microsoft Internet Explorer Multiple Vulnerabilities (2792100)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903300
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS13-009.
Vulnerability Insight:
- An error when handling the encoding for Shift_JIS auto-selection can be
exploited to gain access to information in another domain or Internet
Explorer zone.
- Multiple use-after-free error related to,
SetCapture
COmWindowProxy
CMarkup
vtable
LsGetTrailInfo
CDispNode
pasteHTML
SLayoutRun
InsertElement
CPasteCommand
CObjectElement and
CHTML.
Impact:
Successful exploitation will allow the attackers to gain information of
another domain or Internet Explorer zone and execution of arbitrary code.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-009
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (c) 2013 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 113 $

Serious:

Microsoft Internet Explorer VML Remote Code Execution Vulnerability (2797052)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903301
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS13-010.
Vulnerability Insight:
The flaw is due to an unspecified error when handling certain VML data and
can be exploited to corrupt memory.
Impact:
Successful exploitation will allow attackers to execute arbitrary code and
failed attacks will cause denial of service.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-010
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (c) 2013 SecPod
Summary: Check for the vulnerable 'Vgx.dll' file version
Version: $Revision: 11 $

Serious:

Microsoft Internet Explorer Multiple Use After Free Vulnerabilities (2809289)
Risk:Serious
Application:general
Port:0
Protocol:tcp
ScriptID:903303
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS13-021.
Vulnerability Insight:
Multiple use-after-free error exist in the following functions,
- OnResize
- saveHistory
- CMarkupBehaviorContext
- CCaret
- CElement
- GetMarkupPtr
- onBeforeCopy
- removeChild
- CTreeNode
Impact:
Successful exploitation will allow attackers to corrupt memory by the
execution of arbitrary code in the context of the current user.
Impact Level: System/Application
Affected Software/OS:
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-021
CVSS Base Score : 9.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (c) 2013 SecPod
Summary: Check for the vulnerable 'Mshtml.dll' file version
Version: $Revision: 113 $

High:

Microsoft Remote Desktop Protocol Security Advisory (2861855)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:803867
Summary:
This host is missing an important security update according to Microsoft advisory (2861855).
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
The flaw is due to security issue in Network-level Authentication (NLA) method in Remote Desktop Sessions.
Impact:
Successful exploitation will allow remote attackers to bypass the security.
Affected Software/OS:
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/advisory/2861855
CVSS Base Score : 7.8
Family name: Windows
Category: infos
Copyright: Copyright (c) 2013 SecPod
Summary: Check for the vulnerable 'Tssecsrv.sys' file version
Version: $Revision: 11 $

High:

Microsoft Windows Network Policy Server Denial-of-Service Vulnerability (3014029)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:805241
NODESC
CVSS Base Score : 7.8
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 921 $

High:

Microsoft Windows TCP/IP Stack Denial of Service Vulnerability (2563894)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:900296
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-064.
Vulnerability Insight:
The flaws are due to errors the TCP/IP stack,
- when parsing specially crafted URLs.
- when processing a sequence of specially crafted ICMP messages.
Impact:
Successful exploitation could allow remote attacker to cause the system to
stop responding and automatically restart.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-064.mspx
CVSS Base Score : 7.8
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'tcpip.sys' file version
Version: $Revision: 13 $

High:

Microsoft Windows SMB Server Remote Code Execution Vulnerability (2536275)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902440
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-048.
Vulnerability Insight:
The flaw is caused when Microsoft Server Message Block (SMB) protocol
software improperly handles SMB packets, including some pre-authentication
scenarios.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary code
and cause a denial of service or compromise a vulnerable system.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows Vista Service Pack 1/2 and prior
Microsoft Windows Server 2008 Service Pack 1/2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/Bulletin/MS11-048.mspx
CVSS Base Score : 7.8
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the version of Srvnet.sys file
Version: $Revision: 13 $

High:

Microsoft Windows TCP/IP Denial of Service Vulnerability (2790655)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902945
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-018.
Vulnerability Insight:
The flaw is due to an error within the TCP/IP stack, which remains in
TCP FIN_WAIT_2 state after receiving an ACK to the FIN packet when
handling a tear down sequence.
Impact:
Successful exploitation could allow attackers to exhaust the non-paged pool
and render the system unusable or trigger a restart.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-018
CVSS Base Score : 7.8
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'tcpip.sys' file version
Version: $Revision: 113 $

High:

Microsoft Windows ICMPv6 Packet Denial of Service Vulnerability (2868623)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903316
Summary:
This host is missing a important security update according to Microsoft
Bulletin MS13-065.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Flaw is due to an error within the TCP/IP stack when handling ICMPv6 packets.
Impact:
Successful exploitation will allow attackers to cause denial of service
condition.
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-065
CVSS Base Score : 7.8
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (c) 2013 SecPod
Summary: Check for the vulnerable 'tcpip.sys' file version
Version: $Revision: 11 $

High:

Microsoft Windows On-Screen Keyboard Privilege Escalation Vulnerability (2975685)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:804472
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS14-039
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
The flaw is triggered when executing the On-Screen keyboard from within the
context of a low integrity process.
Impact:
Successful exploitation will allow remote attackers to gain escalated
privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 8 x32/x64
Windows 8.1 x32/x64 Edition
Microsoft Windows Server 2012/R2
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Solution:
Run Windows Update and update the listed hotfixes or download and update
mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms14-039
CVSS Base Score : 7.6
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 758 $

High:

Windows Fax Cover Page Editor Remote Code Execution Vulnerability (2527308)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902408
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-024.
Vulnerability Insight:
The flaw is due to error in fax cover page editor, when user opened a
specially crafted fax cover page file (.cov) using the windows fax cover page
editor will trigger a memory corruption error in the Fax Cover Page Editor
(fxscover.exe) and execute arbitrary code on the target system.
Impact:
Successful exploitation could allow attackers to gain the same user rights as
the logged-on user. Users whose accounts are configured to have fewer user
rights on the system could be less impacted than users who operate with
administrative user rights.
Impact Level: System/Application
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-024.mspx
CVSS Base Score : 7.6
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'fxscover.exe' and 'Mfc42.dll' file version
Version: $Revision: 13 $

High:

Microsoft WinVerifyTrust Signature Validation Vulnerability (2893294)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903228
Summary:
This host is missing an critical security update according to Microsoft Bulletin MS13-098.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Flaw is due to WinVerifyTrust function which does not properly handles the Windows Authenticode signature verification for portable executable(PE) files.
Impact:
Successful exploitation will allow attackers to execute arbitrary code or cause a denial of service condition.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
Microsoft Windows 8 x32/x64
Microsoft Windows 8.1 x32/x64
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms13-098
CVSS Base Score : 7.6
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Imagehlp.dll' file version
Version: $Revision: 116 $

High:

Microsoft DNS Resolution Remote Code Execution Vulnerability (2509553)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:900282
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-030.
Vulnerability Insight:
The flaws are due to the way the DNS client handles specially crafted
LLMNR queries.
Impact:
Successful exploitation could allow remote attacker to execute arbitrary
code in the context of the NetworkService account.
Impact Level: System
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2003 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-030.mspx
CVSS Base Score : 7.5
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Dnsrslvr.dll' file version
Version: $Revision: 13 $

High:

Microsoft Windows Kernel Privilege Elevation Vulnerabilities (2859537)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902990
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-063.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Multiple flaws are due to,
- An error within Address Space Layout Randomization (ASLR) implementation
can be exploited to bypass the ASLR security feature.
- Multiple error within the NT Virtual DOS Machine (NTVDM) subsystem.
Impact:
Successful exploitation will allow remote attackers to execute arbitrary
code with kernel-mode privileges and or corrupt memory.
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows 2003 x32 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update
mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-063
CVSS Base Score : 7.5
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'ntoskrnl.exe' file version
Version: $Revision: 11 $

High:

Microsoft .NET Framework Authentication Bypass and Spoofing Vulnerabilities (2836440)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903308
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-040.
Vulnerability Insight:
The flaws are due to
- Improper validation of XML signatures by the CLR
- Error within the WCF endpoint authentication mechanism when handling
queries
Impact:
Successful exploitation could allow an attacker to bypass security mechanism
and gain access to restricted endpoint functions.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework 4
Microsoft .NET Framework 4.5
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 2.0 Service Pack 2
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-040
CVSS Base Score : 7.5
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the version of 'System.Security.dll' file
Version: $Revision: 11 $

High:

Microsoft Windows Shell Handler Privilege Escalation Vulnerability (2962488)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:804295
Summary:
This host is missing an important security update according to Microsoft Bulletin MS14-027.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Flaw is due to an error in the 'ShellExecute' function within the Windows Shell API when handling file associations.
Impact:
Successful exploitation will allow attackers to gain elevated privileges and execute code in the context of the LocalSystem account.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 8 x32/x64
Microsoft Windows 8.1 x32/x64
Microsoft Windows Server 2012
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-027
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable file version
Version: $Revision: 758 $

High:

Microsoft Windows Kernel Privilege Escalation Vulnerabilities (2930275)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:804409
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS14-015
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Multiple flaws are due to an information disclosure and an elevation of
privilege vulnerabilities exists when the Windows kernel-mode driver improperly
handles objects in memory.
Impact:
Successful exploitation will allow remote attackers to cause a DoS (Denial of
Service) and gain escalated privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 8
Windows 8.1 x32/x64 Edition
Microsoft Windows Server 2012
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update
mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms14-015
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 758 $

High:

Microsoft Windows FAT32 Disk Partition Driver Privilege Escalation Vulnerability (2998579)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:804493
NODESC
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: NOSUMMARY
Version: $Revision: 787 $

High:

MS Windows Ancillary Function Driver Elevation of Privilege Vulnerability (2975684)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:804671
Summary:
This host is missing a critical security update according to Microsoft Bulletin MS14-040.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Flaw is due to a double-free error in the Ancillary Function Driver within 'afd.sys'.
Impact:
Successful exploitation will allow attackers to gain elevated privileges and execute arbitrary code and take complete control of an affected system.
Impact Level: System
Affected Software/OS:
Microsoft Windows 2003 x32 Service Pack 3 and prior
Microsoft Windows 2003 x64 Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
Microsoft Windows 8 x32/x64
Microsoft Windows 8.1 x32/x64
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/ms14-040
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Afd.sys' file version
Version: $Revision: 758 $

High:

MS Windows Kernel-Mode Drivers Privilege Escalation Vulnerabilities (2984615)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:804807
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS14-045
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Multiple flaws exist due to,
- An error within win32k.sys when handling window handle thread-owned objects.
- A double fetch error within win32k.sys when processing font files.
- An error related to Windows kernel pool.
Impact:
Successful exploitation will allow attackers to disclose certain sensitive
information and gain escalated privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows 8 x32/x64
Windows 8.1 x32/x64 Edition
Microsoft Windows Server 2012/R2
Solution:
Run Windows Update and update the listed hotfixes or download and update
mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms14-045
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 758 $

High:

Microsoft Windows Installer Service Privilege Escalation Vulnerarbility (2962490)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:804808
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS14-049
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Flaw exists due to an error within the Windows Installer Service when handling
a repair of a previously installed application
Impact:
Successful exploitation will allow attackers to gain escalated privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows 8 x32/x64
Windows 8.1 x32/x64 Edition
Microsoft Windows Server 2012/R2
Solution:
Run Windows Update and update the listed hotfixes or download and update
mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms14-049
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 758 $

High:

Microsoft Windows User Profile Service Privilege Escalation (3021674)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:805126
NODESC
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 936 $

High:

MS Windows Kernel-Mode Driver RCE Vulnerabilities (3036220)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:805337
NODESC
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1015 $

High:

MS Windows Kernel Privilege Elevation Vulnerabilities (3038680)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:805350
NODESC
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1089 $

High:

MS Windows Kernel-Mode Driver Privilege Elevation Vulnerabilities (3034344)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:805351
NODESC
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1089 $

High:

Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2506223)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:900283
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-034.
Vulnerability Insight:
The flaws are due to improper Kernel-mode driver object management
and Null pointer de-reference due to the way kernel-mode drivers keep track
of pointers to certain kernel-mode driver objects.
Impact:
Successful exploitation could allow local attackers to gain elevated
privileges.
Impact Level: System/Application
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-034.mspx
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 13 $

High:

Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2479628)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:901182
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-012.
Vulnerability Insight:
The flaws are caused by input validation errors, improper pointer validation,
pointer confusions, and memory corruption errors in the Windows kernel-mode
drivers 'win32k.sys' when processing data supplied from user mode to kernel
mode, which could allow malicious users to execute arbitrary code with kernel
privileges.
Impact:
Successful exploitation could allow local attackers to gain elevated
privileges.
Impact Level: System/Application
Affected Software/OS:
Micorsoft Windows 7
Microsoft Windows XP Service Pack 3 and prior.
Microsoft Windows 2K3 Service Pack 2 and prior.
Microsoft Windows Vista Service Pack 2 and prior.
Microsoft Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-012.mspx
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 13 $

High:

Microsoft Windows Kernel Elevation of Privilege Vulnerability (2393802)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902337
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-011.
Vulnerability Insight:
The flaws are due to
- an integer truncation error in the Windows kernel that does not properly
validate user-supplied data before allocating memory.
- a buffer overflow error in the 'win32k.sys' driver when interacting with
the Windows kernel.
Impact:
Successful exploitation will allow remote attackers or malicious users to
execute arbitrary code with kernel privileges.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 7
Microsoft Windows XP Service Pack 3 and prior.
Microsoft Windows 2K3 Service Pack 2 and prior.
Microsoft Windows Vista Service Pack 2 and prior.
Microsoft Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-011.mspx
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the version of 'Ntoskrnl.exe' file
Version: $Revision: 13 $

High:

MS Windows Ancillary Function Driver Privilege Elevation Vulnerability
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902442
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-046.
Vulnerability Insight:
The flaw is caused by an error in Ancillary Function Driver (AFD) which does
not properly validates input before passing the input from user mode to the
Windows kernel.
Impact:
Successful exploitation could allow elevation of privilege if an attacker
logs on to a user's system and runs a specially crafted application.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-046.mspx
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Afd.sys' file version
Version: $Revision: 13 $

High:

Microsoft Windows Client/Server Run-time Subsystem Privilege Escalation Vulnerability (2567680)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902463
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-063.
Vulnerability Insight:
The flaw is due to error in the Client/Server Run-time Subsystem
(CSRSS) when evaluates inter-process device event message permissions.
Impact:
Successful exploitation could allow attacker to execute arbitrary code with
system-level privileges. Successfully exploiting this issue will result in
the complete compromise of affected computers.
Impact Level: System
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior.
Microsoft Windows XP Service Pack 3 and prior.
Microsoft Windows 2003 Service Pack 2 and prior.
Microsoft Windows Vista Service Pack 2 and prior.
Microsoft Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-063.mspx
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'winsrv.dll' and 'Kernel32.dll' files version
Version: $Revision: 13 $

High:

Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2555917)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902538
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-054.
Vulnerability Insight:
The flaws are due to improper Kernel-mode driver object management
and Null pointer de-reference due to the way kernel-mode drivers keep track
of pointers to certain kernel-mode driver objects.
Impact:
Successful exploitation could allow local attackers to gain elevated
privileges.
Impact Level: System/Application
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2003 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-054.mspx
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 13 $

High:

Microsoft Windows CSRSS Privilege Escalation Vulnerabilities (2507938)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902609
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-056.
Vulnerability Insight:
The flaws are due to,
- memory corruption error related to AllocConsole
- memory corruption error related to SrvSetConsoleLocalEUDC
- improper verification by SrvSetConsoleNumberOfCommand
- integer overflow in SrvWriteConsoleOutput
Impact:
Successful exploitation could allow local attacker to execute arbitrary
code on the system with elevated privileges.
Impact Level: System
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2003 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-056.mspx
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'winsrv.dll' file version
Version: $Revision: 13 $

High:

Windows Client/Server Run-time Subsystem Privilege Elevation Vulnerability (2620712)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902643
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-097.
Vulnerability Insight:
The flaw is caused by an error in the Client/Server Run-time Subsystem(CSRSS)
when evaluating inter-process device event message permissions, which could
allow a low integrity process to send message to a higher integrity process.
Impact:
Successful exploitation could allow local attackers to obtain sensitive
information or gain privileges when runnin with administrator privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-097
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Csrsrv.dll' file version
Version: $Revision: 13 $

High:

Microsoft Windows TCP/IP Privilege Elevation Vulnerabilities (2688338)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902676
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS12-032.
Vulnerability Insight:
The flaws are due to the way,
- Windows Firewall handles outbound broadcast packets.
- Windows TCP/IP stack handles the binding of an IPv6 address to a local
interface.
Impact:
Successful exploitation could allow attackers to bypass certain security
restrictions and gain escalated privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows Server 2008 R2 Service Pack 1
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-032
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'tcpip.sys' file version
Version: $Revision: 110 $

High:

Microsoft Windows Prtition Manager Privilege Elevation Vulnerability (2690533)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902677
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS12-033.
Vulnerability Insight:
The flaw is due to the way Windows Partition Manager (partmgr.sys)
allocates objects in memory, when two or more processes or threads call
Plug and Play (PnP) Configuration Manager functions at the same time.
Impact:
Successful exploitation could allow attackers to gain escalated privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Microsoft Windows Server 2008 R2 Service Pack 1 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-033
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Partmgr.sys' file version
Version: $Revision: 110 $

High:

Microsoft Windows Kernel Privilege Elevation Vulnerability (2633171)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902766
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-098.
Vulnerability Insight:
The flaw is caused due an error within certain exception handlers in the
kernel when handling objects.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code with kernel-mode privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-098
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'ntoskrnl.exe' file version
Version: $Revision: 13 $

High:

Windows Kernel-Mode Drivers Privilege Elevation Vulnerability (2641653)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902907
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS12-018.
Vulnerability Insight:
The flaw is due to an error in win32k.sys when handling the 'PostMessage()'
function and can be exploited via an application passing specially crafted input
to the function.
Impact:
Successful exploitation could allow local attackers to gain escalated
privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2003 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-018
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 12 $

High:

Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2709162)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902917
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS12-041.
Vulnerability Insight:
Multiple flaws are due to,
- An error in win32k.sys within the string atom class name and lipboard format atom name handling and can be exploited to execute arbitrary code.
- An integer overflow error when handling the reference counter for font resources when loading TrueType fonts.
- A race condition error in win32k.sys when handling particular thread creation attempts and can be exploited to execute arbitrary code.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary code with kernel-mode privileges
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-041
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 12 $

High:

Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerability (2778930)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902938
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-005.
Vulnerability Insight:
The flaw is due to an error in 'win32k.sys' when handling window broadcast
messages.
Impact:
Successful exploitation will allow remote attackers to gain escalated
privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-005
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 113 $

High:

Microsoft Windows Kernel Privilege Elevation Vulnerabilities (2799494)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902944
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-017.
Vulnerability Insight:
- Race condition errors when handling certain objects in memory can be
exploited to execute arbitrary code with kernel privileges.
- An error when handling the reference counter for certain objects in memory
can be exploited to execute arbitrary code with kernel privileges.
Impact:
Successful exploitation will allow remote attackers to execute arbitrary
code with kernel-mode privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-017
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'ntoskrnl.exe' file version
Version: $Revision: 11 $

High:

MS Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2876315)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902994
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-076.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Multiple flaws are due to error related to multiple fetch within the
kernel-mode driver (win32k.sys).
Impact:
Successful exploitation will allow remote attackers to gain escalated
privileges, read arbitrary kernel memory and cause a DoS (Denial of
Service).
Impact Level: System
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update
mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-076
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 11 $

High:

Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2718523)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903033
Summary:
This host has important security update missing according to
Microsoft Bulletin MS12-047.
Vulnerability Insight:
Windows kernel-mode driver improperly validates parameters (when creating a
hook procedure) and specific keyboard layouts, which can be exploited to
execute arbitrary code.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code with kernel-mode privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-047
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 12 $

High:

Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerability (2731847)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903035
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS12-055.
Vulnerability Insight:
The flaw is due to a use-after-free error in win32k.sys when
accessing objects in memory.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code with kernel-mode privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-055
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 12 $

High:

Microsoft Windows Kernel Privilege Elevation Vulnerability (2724197)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903041
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS12-068.
Vulnerability Insight:
The flaw is due to an integer overflow error when handling certain
objects in memory and can be exploited to execute arbitrary code with
kernel privileges.
Impact:
Successful exploitation could allow remote attackers to execute arbitrary
code with kernel-mode privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-068
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'ntoskrnl.exe' file version
Version: $Revision: 110 $

High:

Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2807986)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903200
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-027.
Vulnerability Insight:
Multiple flaws are due to improper handling of objects in memory by the
kernel-mode driver, which can be exploited by inserting a malicious USB
device into the system.
Impact:
Successful exploitation could allow remote attackers to compromise the
affected system and possibly execute arbitrary code with System-level
privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/MS13-027
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Usb8023.sys' file version
Version: $Revision: 11 $

High:

MS Windows Client/Server Run-time Subsystem Privilege Escalation Vulnerability (2820917)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903205
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-033.
Vulnerability Insight:
The flaw is due to an improper sanitation of user-supplied input when
handling certain objects in memory.
Impact:
Successful exploitation will allow attackers to execute arbitrary code,
gain escalated privileges, and cause memory corruption.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-033
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Winsrv.dll' file version
Version: $Revision: 11 $

High:

Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2840221)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903208
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-046.
Vulnerability Insight:
Multiple flaws are due to,
- A race condition error within the DirectX graphics kernel subsystem.
- An unspecified error within the Windows kernel-mode driver (win32k.sys)
Impact:
Successful exploitation will allow remote attackers to gain escalated
privileges or cause buffer overflow and execute arbitrary code.
Impact Level: System
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-046
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'Win32k.sys', Ntoskrnl.exe and 'Dxgkrnl.sys' file version
Version: $Revision: 11 $

High:

Microsoft Windows Kernel Local Privilege Escalation Vulnerabilities (2880430)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903417
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-101
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Multiple flaws are due to ,
- An error within the win32k.sys driver can be exploited to corrupt memory.
- A use-after-free error exists within the win32k.sys driver.
- An error when processing TrueType font files can be exploited to cause
a crash.
- A double fetch error exists within the portcls.sys driver.
- An integer overflow error exists within the win32k.sys driver.
Impact:
Successful exploitation will allow remote attackers to cause a DoS (Denial of
Service) and gain escalated privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 8
Windows 8.1 x32/x64 Edition
Microsoft Windows Server 2012
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update
mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-101
CVSS Base Score : 7.2
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable files version
Version: $Revision: 116 $

High:

Microsoft DirectAccess Security Advisory (2862152)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:804143
Summary:
This host is missing an important security update according to Microsoft advisory (2862152).
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
The flaw is due to improper verification of DirectAccess server connections to DirectAccess clients by DirectAccess.
Impact:
Successful exploitation will allow an attacker to intercept the target user's network traffic and potentially determine their encrypted domain credentials.
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows 8.1 x32/x64
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/advisory/2862152
CVSS Base Score : 7.1
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable file version
Version: $Revision: 75 $

High:

MS Windows Kernel-Mode Driver TrueType Font DoS Vulnerability (3002885)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:804878
NODESC
CVSS Base Score : 7.1
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 818 $

High:

Microsoft Windows Kernel-Mode Driver Denial of Service Vulnerability (2845690)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902975
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-049.
Vulnerability Insight:
The flaw is due to an integer overflow error within Windows TCP/IP driver
when handling packets during TCP connection, which can be exploited to
cause the system to stop responding.
Impact:
Successful exploitation could allow attackers to cause a denial of service.
Impact Level: System
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-049
CVSS Base Score : 7.1
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'tcpip.sys' file version
Version: $Revision: 11 $

High:

Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2829996)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903202
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-036.
Vulnerability Insight:
Multiple flaws are due to,
- Improper handling of certain objects in kernel memory.
- Improper parsing of crafted OpenType font files.
Impact:
Successful exploitation will allow remote attackers to gain escalated
privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-036
CVSS Base Score : 7.1
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Win32k.sys' and 'Ntfs.sys' file version
Version: $Revision: 113 $

High:

Microsoft Window XML Core Services Information Disclosure Vulnerability (2916036)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903510
Summary:
This host is missing an important security update according to Microsoft Bulletin MS14-005.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
The flaw is due to an unspecified error which improperly enforce cross-domain policies.
Impact:
Successful exploitation will allow remote attackers to read files on the local file system of the user or read content of web domains where the user is currently authenticated.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 8 x32/x64
Microsoft Windows 8.1 x32/x64
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-005
CVSS Base Score : 7.1
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 SecPod
Summary: Check for the vulnerable 'Msxml3.dll' file version
Version: $Revision: 271 $

High:

MS Windows HID Functionality(Over USB) Code Execution Vulnerability
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:801581
Summary:
This host is installed with USB device driver software and is
prone to code execution vulnerability.
Vulnerability Insight:
The flaw is due to error in USB divice driver, which does not
properly warn the user before enabling additional Human Interface Device (HID)
functionality.
Impact:
Successful exploitation will allows user-assisted attackers to
execute arbitrary programs via crafted USB data.
Impact Level: System/Application
Affected Software/OS:
Micorsoft Windows 7
Microsoft Windows XP Service Pack 2 and prior
Microsoft Windows 2k Service Pack 4 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows 2k8 Service Pack 4 and prior
Microsoft Windows Vista service Pack 2 and prior
Solution:
No solution or patch was made available for at least one year
since disclosure of this vulnerability. Likely none will be provided anymore.
General solution options are to upgrade to a newer release, disable respective
features, remove the product or replace the product by another one.
CVSS Base Score : 6.9
Family name: Windows
Category: infos
Copyright: Copyright (c) 2011 Greenbone Networks GmbH
Summary: Check for the existance of hidserv.dll file
Version: $Revision: 267 $

High:

Microsoft File Handling Component Remote Code Execution Vulnerability (2922229)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:804375
Summary:
This host is missing an important security update according to Microsoft
Bulletin MS14-019.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Flaw is due to an improper path restrictions when processing .bat and .cmd
files related to the 'CreateProcess' function.
Impact:
Successful exploitation will allow attackers to execute arbitrary code and
potentially compromise user's system.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 8 x32/x64
Microsoft Windows 8.1 x32/x64
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows XP x64 Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms14-019
CVSS Base Score : 6.9
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable 'kernel32.dll' file version
Version: $Revision: 758 $

High:

Microsoft Digital Certificates Security Advisory (2916652)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:803978
Summary:
This host is missing an important security update according to Microsoft advisory (2916652).
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
The flaw is due to DG Tresor which improperly issued a subordinate CA certificate
Impact:
Successful exploitation will allow attackers to to spoof content, perform phishing attacks, or perform man-in-the-middle attacks.
Impact Level: Application
Affected Software/OS:
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link
https://technet.microsoft.com/en-us/security/advisory/2916652
CVSS Base Score : 6.8
Family name: Windows
Category: infos
Copyright: Copyright (C) 2013 Greenbone Networks GmbH
Summary: Check for the vulnerable 'Crypt32.dll' file version
Version: $Revision: 992 $

High:

Microsoft Update to Improve Cryptography and Digital Certificate Handling (2854544)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903310
Summary:
This host is missing an important security update according to
Microsoft Security Advisory (2854544).
Vulnerability Insight:
The flaw is due to a Flame modules named 'Gadget' and 'Munch', used to infect
other machines in the same network as the targeted machine.
Impact:
Successful exploitation could allow remote attackers to perform
man-in-the-middle attack during a Windows Update session that basically
redirects the user's machine to a phony update with the malware.
Impact Level: System
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/advisory/2854544
CVSS Base Score : 6.8
Family name: Windows
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Crypt32.dll' file version
Version: $Revision: 11 $

High:

MS Windows Network Location Awareness Service Security Bypass Vulnerability (3022777)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:805036
NODESC
CVSS Base Score : 6.1
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 936 $

High:

Microsoft Windows Security Feature Bypass Vulnerability (2785220)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:901214
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-006.
Vulnerability Insight:
The vulnerability is caused when Windows fails to properly handle SSL/TLS
session version negotiation.
Impact:
Successful exploitation could allow remote attackers to silently downgrade
a SSL version 3 or TLS connection to SSL version 2, which supports weak
encryption cyphers.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-006
CVSS Base Score : 5.8
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Ncrypt.dll' file version
Version: $Revision: 141 $

High:

Microsoft Windows SAMR Protocol Security Bypass Vulnerability (2934418)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:804245
Summary:
This host is missing an important security update according to Microsoft Bulletin MS14-016.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
Flaw is due to improper validation of user lockout state by Security Account Manager Remote (SAMR) protocol .
Impact:
Successful exploitation will allow attackers to bypass certain security features.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-016
CVSS Base Score : 5.4
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable version of files
Version: $Revision: 758 $

High:

Microsoft Windows Netlogon Service Denial of Service Vulnerability (2207559)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902277
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS10-101.
Vulnerability Insight:
The issue is caused by an error in the Netlogon RPC Service when processing
user-supplied data, which could allow attackers to crash an affected server
that is configured as a domain controller.
Impact:
Successful exploitation will allows attackers to cause a denial of service.
Impact Level: System/Application
Affected Software/OS:
Windows Server 2003 Service Pack 2 and prior.
Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/Bulletin/MS10-101.mspx
CVSS Base Score : 5.4
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2010 SecPod
Summary: Check for the version of Netlogon.dll file
Version: $Revision: 14 $

High:

Microsoft .NET Framework Remote Code Execution Vulnerability (2538814)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:902522
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-044.
Vulnerability Insight:
The flaw is due to the JIT compiler, when IsJITOptimizerDisabled is
false, does not properly handle expressions related to null strings, which
allows context-dependent attackers to bypass intended access restrictions.
Impact:
Successful exploitation could allow context-dependent attackers to bypass
intended access restrictions in opportunistic circumstances by leveraging
a crafted application.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework 4.0
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 3.5 Service Pack 1
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 2.0 Service Pack 1
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-044
CVSS Base Score : 5.1
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the version of 'mscorlib.dll' file
Version: $Revision: 13 $

High:

DCE Services Enumeration
Risk:High
Application:epmap
Port:135
Protocol:tcp
ScriptID:10736
Summary:
Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.
An attacker may use this fact to gain more knowledge
about the remote host.
Solution:
filter incoming traffic to this port.
CVSS Base Score : 5.0
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2001 Dave Aitel (ported to NASL by rd and Pavel Kankovsky)
Summary: Enumerates the remote DCE services
Version: $Revision: 41 $

High:

DCE Services Enumeration
Risk:High
Application:epmap
Port:135
Protocol:tcp
ScriptID:10736
Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.
An attacker may use this fact to gain more knowledge
about the remote host.
Here is the list of DCE services running on this host:
Port: 49152/tcp
UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
Endpoint: ncacn_ip_tcp:10.47.30.102[49152]
Port: 49153/tcp
UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
Endpoint: ncacn_ip_tcp:10.47.30.102[49153]
Annotation: Event log TCPIP
UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
Endpoint: ncacn_ip_tcp:10.47.30.102[49153]
Annotation: DHCP Client LRPC Endpoint
UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
Endpoint: ncacn_ip_tcp:10.47.30.102[49153]
Annotation: DHCPv6 Client LRPC Endpoint
Port: 49154/tcp
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
Endpoint: ncacn_ip_tcp:10.47.30.102[49154]
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
Endpoint: ncacn_ip_tcp:10.47.30.102[49154]
Annotation: IKE/Authip API
UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
Endpoint: ncacn_ip_tcp:10.47.30.102[49154]
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
Endpoint: ncacn_ip_tcp:10.47.30.102[49154]
Annotation: Impl friendly name
Port: 49155/tcp
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
Endpoint: ncacn_ip_tcp:10.47.30.102[49155]
Port: 49156/tcp
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:10.47.30.102[49156]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : SAM access
Solution : filter incoming traffic to this port(s).
CVSS Base Score : 5.0
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2001 Dave Aitel (ported to NASL by rd and Pavel Kankovsky)
Summary: Enumerates the remote DCE services
Version: $Revision: 41 $

High:

Microsoft Internet Explorer Multiple Information Disclosure Vulnerabilities
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:802286
Summary:
The host is installed with Internet Explorer and is prone to
multiple information disclosure vulnerabilities.
Vulnerability Insight:
Multiple flaws are due to
- The Cascading Style Sheets (CSS) implementation does not properly handle
the :visited pseudo-class, which allows remote attackers to obtain
sensitive information about visited web pages via a crafted HTML document.
- The JavaScript implementation is not properly restrict the set of values
contained in the object returned by the getComputedStyle method, which
allows remote attackers to obtain sensitive information about visited web
pages.
Impact:
Successful exploitation will allow attackers to gain access
to sensitive information and launch other attacks.
Impact Level: Application
Affected Software/OS:
Internet Explorer Version 8 and prior.
Solution:
No solution or patch was made available for at least one year
since disclosure of this vulnerability. Likely none will be provided anymore.
General solution options are to upgrade to a newer release, disable respective
features, remove the product or replace the product by another one.
CVSS Base Score : 5.0
Family name: General
Category: infos

Summary: Check for the version of Internet Explorer
Version: $Revision: 282 $

High:

Microsoft Internet Explorer Cache Objects History Information Disclosure Vulnerability
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:802287
Summary:
The host is installed with Internet Explorer and is prone to
information disclosure vulnerability.
Vulnerability Insight:
The flaw is due to an error when handling cache objects and can
be exploited to enumerate visited sites.
Impact:
Successful exploitation will allow attackers to gain access to
sensitive information and launch other attacks.
Impact Level: Application
Affected Software/OS:
Internet Explorer Versions 6 through 9.
Solution:
No solution or patch was made available for at least one year
since disclosure of this vulnerability. Likely none will be provided anymore.
General solution options are to upgrade to a newer release, disable respective
features, remove the product or replace the product by another one.
CVSS Base Score : 5.0
Family name: General
Category: infos
Copyright: Copyright (C) 2011 Greenbone Networks GmbH
Summary: Check for the version of Internet Explorer
Version: $Revision: 282 $

High:

Microsoft .NET Framework Denial of Service Vulnerability (2990931)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:804480
NODESC
CVSS Base Score : 5.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 787 $

High:

Microsoft Windows TCP Protocol Denial of Service Vulnerability (2962478)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:804636
Summary:
This host is missing an important security update according to Microsoft
Bulletin MS14-031.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Flaw is due to some error within the Windows TCP/IP networking protocol which
allows processing of crafted packets.
Impact:
Successful exploitation will allow attackers to cause denial of service
condition.
Affected Software/OS:
Microsoft Windows 8 x32/x64
Microsoft Windows 8.1 x32/x64
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/library/security/ms14-031
CVSS Base Score : 5.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: Check for the vulnerable 'Tcpip.sys' file version
Version: $Revision: 758 $

High:

MS Windows Remote Desktop Protocol Security Feature Bypass Vulnerability (3003743)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:805017
NODESC
CVSS Base Score : 5.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 818 $

High:

Microsoft Graphics Component Information Disclosure Vulnerability (3013126)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:805207
NODESC
CVSS Base Score : 5.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 992 $

High:

Microsoft Schannel Security Feature Bypass Vulnerability (3046049)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:805490
NODESC
CVSS Base Score : 5.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1076 $

High:

Microsoft Internet Explorer PDF Information Disclosure Vulnerability - Nov09
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:900897
Summary:
This host is installed with Internet Explorer and is prone to
Information Disclosure vulnerability.
Vulnerability Insight:
The weakness is due to an Internet Explorer including the first
63 bytes of the file path in the 'Title' property when converting local HTML or
MHT files to PDF using a PDF printer. This can lead to the exposure of certain
system information e.g. the user name.
Impact:
Successful attacks which may leads to the exposure of system
information on the affected system.
Impact Level: System
Affected Software/OS:
Microsoft Internet Explorer version 6/7/8 on Windows.
Solution:
No solution or patch was made available for at least one year
since disclosure of this vulnerability. Likely none will be provided anymore.
General solution options are to upgrade to a newer release, disable respective
features, remove the product or replace the product by another one.
CVSS Base Score : 5.0
Family name: General
Category: infos
Copyright: Copyright (C) 2009 SecPod
Summary: Check for the version of Internet Explorer
Version: $Revision: 244 $

High:

Microsoft Windows Digital Signatures Denial of Service Vulnerability (2868626)
Risk:High
Application:general
Port:0
Protocol:tcp
ScriptID:903227
Summary:
This host is missing an important security update according to Microsoft
Bulletin MS13-095.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Flaw is caused when Microsoft Windows improperly handles web-service request
containing a crafted X.509 certificate.
Impact:
Successful exploitation will allow attackers to cause a denial of service condition.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
Microsoft Windows 8 x32/x64
Microsoft Windows 8.1 x32/x64
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-095
CVSS Base Score : 5.0
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Crypt32.dll' file version
Version: $Revision: 113 $

Medium:

Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2778344)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:902943
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-016.
Vulnerability Insight:
The flaws due to an error in 'win32k.sys' when handling kernel-mode driver
objects in memory.
Impact:
Successful exploitation will allow remote attackers to a specially crafted
program to exploit race conditions in 'win32k.sys' and gain System level
privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-016
CVSS Base Score : 4.9
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'Win32k.sys' file version
Version: $Revision: 113 $

Medium:

Microsoft Windows Kernel Privilege Elevation Vulnerabilities (2813170)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:902959
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-031.
Vulnerability Insight:
Multiple race condition errors when handling certain objects in memory can be
exploited to execute arbitrary code with kernel privileges.
Impact:
Successful exploitation will allow remote attackers to execute arbitrary
code with kernel-mode privileges.
Impact Level: System
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows Server 2012
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms13-031
CVSS Base Score : 4.9
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'ntoskrnl.exe' file version
Version: $Revision: 113 $

Medium:

Microsoft Windows Kernel Denial of Service Vulnerability (2556532)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:900297
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-068.
Vulnerability Insight:
The flaw is due to an error in the kernel when parsing meta data information
in files.
Impact:
Successful exploitation could allow remote attacker to cause the system to
stop responding or system to restart.
Impact Level: System
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior.
Microsoft Windows Vista Service Pack 2 and prior.
Microsoft Windows Server 2008 Service Pack 2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-068.mspx
CVSS Base Score : 4.7
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'ntoskrnl.exe' file version
Version: $Revision: 13 $

Medium:

Microsoft Windows Kernel Information Disclosure Vulnerability (2839229)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:902974
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS13-048.
Vulnerability Insight:
The weakness is due to an error when handling certain page fault system calls,
which can be exploited to disclose information from kernel memory.
Impact:
Successful exploitation will allow local attackers to disclose potentially
sensitive information.
Impact Level: System
Affected Software/OS:
Microsoft Windows 8
Microsoft Windows 7 x32 Edition Service Pack 1 and prior
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows 2003 x32 Edition Service Pack 2 and prior
Microsoft Windows Vista x32 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 x32 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms13-048
CVSS Base Score : 4.4
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2013 SecPod
Summary: Check for the vulnerable 'ntoskrnl.exe' file version
Version: $Revision: 11 $

Medium:

Microsoft Internet Explorer 'IFRAME' Denial Of Service Vulnerability (June-10)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:801349
Summary:
This host is installed with Internet Explorer and is prone to
Denial Of Service vulnerability.
Vulnerability Insight:
The flaw is due to improper handling of an 'JavaScript' code
which contains an infinite loop, that creates IFRAME elements for invalid
news:// URIs.
Impact:
Successful exploitation will allow remote attackers to cause a
denial of service.
Impact Level: Application
Affected Software/OS:
Microsoft Internet Explorer version 6.0.2900.2180/8.0.7600.16385
and prior.
Solution:
No solution or patch was made available for at least one year
since disclosure of this vulnerability. Likely none will be provided anymore.
General solution options are to upgrade to a newer release, disable respective
features, remove the product or replace the product by another one.
CVSS Base Score : 4.3
Family name: Denial of Service
Category: infos
Copyright: Copyright (c) 2010 Greenbone Networks GmbH
Summary: Check for the version of Internet Explorer
Version: $Revision: 255 $

Medium:

Microsoft Windows Unauthorized Digital Certificates Spoofing Vulnerability (2718704)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:802634
Summary:
The host is installed with Microsoft Windows operating system and
is prone to digital certificates spoofing vulnerability.
Vulnerability Insight:
The flaw is due to unauthorized digital certificates derived from a Microsoft
Certificate Authority. An unauthorized certificate could be used to spoof
content, perform phishing attacks, or perform man-in-the-middle attacks.
Impact:
Successful exploitation will allow remote attackers to spoof content, perform
phishing attacks or perform man-in-the-middle attacks.
Impact Level: System
Affected Software/OS:
Windows 7 Service Pack 1 and prior
Windows XP Service Pack 3 and prior
Windows Vista Service Pack 2 and prior
Windows Server 2003 Service Pack 2 and prior
Windows Server 2008 Service Pack 2 and prior
Solution:
Apply the Patch from below link,
http://technet.microsoft.com/en-us/security/advisory/2718704
CVSS Base Score : 4.3
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH
Summary: Check for the vulnerable certificates
Version: $Revision: 12 $

Medium:

Microsoft Windows Minimum Certificate Key Length Spoofing Vulnerability (2661254)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:803007
Summary:
The host is installed with Microsoft Windows operating system and
is prone to digital certificate key length spoofing vulnerability.
Vulnerability Insight:
The private keys used in digital certificate with RSA keys less than 1024
bits in length can be derived and could allow an attacker to duplicate the
certificates. An duplicate certificate could be used to spoof content,
perform phishing attacks, or perform man-in-the-middle attacks.
Impact:
Successful exploitation will allow remote attackers to spoof content, perform
phishing attacks or perform man-in-the-middle attacks.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Apply the Patch from below link,
http://technet.microsoft.com/en-us/security/advisory/2661254
CVSS Base Score : 4.3
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH
Summary: Check for the vulnerable Crypt32.dll file version
Version: $Revision: 12 $

Medium:

Microsoft Window XML Core Services Information Disclosure Vulnerability (2966061)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:804635
Summary:
This host is missing an important security update according to Microsoft Bulletin MS14-033.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied or not.
Vulnerability Insight:
The flaw is due to an error when parsing XML entities that is triggered when handling specially crafted XML content on a webpage.
Impact:
Successful exploitation will allow remote attackers to disclose sensitive information.
Impact Level: Application
Affected Software/OS:
Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Service Pack 2 and prior
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
Microsoft Windows 8 x32/x64
Microsoft Windows 8.1 x32/x64
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Solution:
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/library/security/ms14-033
CVSS Base Score : 4.3
Family name: Windows : Microsoft Bulletins
Category: infos

Summary: Check for the vulnerable file version
Version: $Revision: 758 $

Medium:

Microsoft .NET Framework Security Bypass Vulnerability (2984625)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:804740
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS14-046.
Vulnerability Detection:
Get the vulnerable file version and check appropriate patch is applied
or not.
Vulnerability Insight:
Flaw is triggered when handling specially crafted website content due to the
Address Space Layout Randomization (ASLR) security feature.
Impact:
Successful exploitation could allow an attacker to execute of arbitrary code
and bypass certain security mechanism.
Affected Software/OS:
Microsoft .NET Framework 2.0 Service Pack 2, 3.0 Service Pack 2, 3.5, 3.5.1
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/en-us/security/bulletin/ms14-046
CVSS Base Score : 4.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 758 $

Medium:

Microsoft Window Audio Service Privilege Escalation Vulnerability (3005607)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:804880
NODESC
CVSS Base Score : 4.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 818 $

Medium:

Microsoft Graphics Component Information Disclosure Vulnerability (3029944)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:805137
NODESC
CVSS Base Score : 4.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1015 $

Medium:

Microsoft Windows NETLOGON Spoofing Vulnerability (3002657)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:805145
NODESC
CVSS Base Score : 4.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1089 $

Medium:

Microsoft PNG Processing Information Disclosure Vulnerability (3035132)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:805489
NODESC
CVSS Base Score : 4.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1089 $

Medium:

Microsoft Windows Photo Decoder Information Disclosure Vulnerability (3035126)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:805501
NODESC
CVSS Base Score : 4.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1089 $

Medium:

Microsoft IE cross-domain IFRAME gadgets keystrokes steal Vulnerability
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:902210
Summary:
This host is installed with Internet Explorer and is prone to
cross-domain iframe gadgets keystrokes steal vulnerability.
Vulnerability Insight:
The flaw is due to improper handling of 'top.focus()' function,
which does not properly restrict focus changes, which allows remote attackers to
read keystrokes via 'cross-domain IFRAME gadgets'
Impact:
Successful exploitation will allow cross-domain iframe gadgets
to steal keystrokes (including password field entries) transparently.
Impact Level: Application
Affected Software/OS:
Microsoft Internet Explorer version 8.0.7600.16385 and prior.
Solution:
No solution or patch was made available for at least one year
since disclosure of this vulnerability. Likely none will be provided anymore.
General solution options are to upgrade to a newer release, disable respective
features, remove the product or replace the product by another one.
CVSS Base Score : 4.3
Family name: General
Category: infos
Copyright: Copyright (c) 2010 SecPod
Summary: Check for the version of Internet Explorer
Version: $Revision: 256 $

Medium:

Windows MHTML Information Disclosure Vulnerability (2503658)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:902409
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS11-026.
Vulnerability Insight:
The flaw is caused by an error in the way MHTML (MIME Encapsulation of Aggregate
HTML) interprets MIME-formatted requests for content blocks within a document,
which could allow attackers to inject a client-side script in the response of a
web request run in the context of Internet Explorer by tricking a user into
following a specially crafted 'MHTML:' link.
Impact:
Successful exploitation could allow attackers to gain knowledge of sensitive
information.
Impact Level: System/Application
Affected Software/OS:
Micorsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-026.mspx
CVSS Base Score : 4.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Inetcomm.dll' file version
Version: $Revision: 13 $

Medium:

Windows MHTML Information Disclosure Vulnerability (2544893)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:902441
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-037.
Vulnerability Insight:
The flaw is caused by an error in the way MHTML (MIME Encapsulation of Aggregate
HTML) interprets MIME-formatted requests for content blocks within a document,
which could allow attackers to inject a client-side script in the response of a
web request run in the context of Internet Explorer by tricking a user into
following a specially crafted 'MHTML:' link.
Impact:
Successful exploitation could allow attackers to gain knowledge of sensitive
information.
Impact Level: Application
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms11-037.mspx
CVSS Base Score : 4.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the vulnerable 'Inetcomm.dll' file version
Version: $Revision: 13 $

Medium:

Microsoft .NET Framework Information Disclosure Vulnerability (2567951)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:902551
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS11-069.
Vulnerability Insight:
The flaw is due to an error when validating the trust level within
the System.Net.Sockets namespace and can be exploited to bypass CAS (Code
Access Security) restrictions or disclose information via a specially
crafted web page viewed using a browser that supports XBAPs (XAML Browser
Applications).
Impact:
Successful exploitation could allow attacker to bypass certain security
restrictions or gain knowledge of sensitive information.
Impact Level: System/Application
Affected Software/OS:
Microsoft .NET Framework 4.0
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 2.0 Service Pack 2
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms11-069
CVSS Base Score : 4.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2011 SecPod
Summary: Check for the version of 'System.dll' file
Version: $Revision: 13 $

Medium:

Microsoft Windows TLS Protocol Information Disclosure Vulnerability (2655992)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:902846
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS12-049.
Vulnerability Insight:
Microsoft Windows contains a flaw related to the Transport Layer Security
(TLS) Handshake Protocol when the Cipher-block chaining (CBC) mode of
operation is used. This flaw may allow a remote attacker to gain access to
decrypted traffic.
Impact:
Successful exploitation could allow an attacker to gain access to sensitive
information that may aid in further attacks.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-049
CVSS Base Score : 4.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'Schannel.dll' file version
Version: $Revision: 12 $

Medium:

Microsoft Windows SSL/TLS Information Disclosure Vulnerability (2643584)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:902900
Summary:
This host is missing an important security update according to
Microsoft Bulletin MS12-006.
Vulnerability Insight:
A flaw exists is due to an error in Microsoft Windows SChannel (Secure Channel),
when modifying the way that the Windows Secure Channel (SChannel) component
sends and receives encrypted network packets.
Impact:
Successful exploitation of this issue may allow attackers to perform limited
man-in-the-middle attacks to inject data into the beginning of the
application protocol stream to execute HTTP transactions, bypass
authentication.
Impact Level: Windows
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior.
Microsoft Windows XP Service Pack 3 and prior.
Microsoft Windows 2K3 Service Pack 2 and prior.
Microsoft Windows Vista Service Pack 1/2 and prior.
Microsoft Windows Server 2008 Service Pack 1/2 and prior.
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-006
CVSS Base Score : 4.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable file version
Version: $Revision: 12 $

Medium:

Microsoft Windows DirectWrite Denial of Service Vulnerability (2665364)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:902908
Summary:
This host has moderate security update missing according to
Microsoft Bulletin MS12-019.
Vulnerability Insight:
The flaw is due to an error in DirectWrite and can be exploited to
cause an application using the API to stop responding via a specially crafted
sequence of unicode characters.
Impact:
Successful exploitation could allow remote attackers to cause a denial
of service.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://technet.microsoft.com/en-us/security/bulletin/ms12-019
CVSS Base Score : 4.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Check for the vulnerable 'D3d10_1.dll'and 'Dwrite.dll' file version
Version: $Revision: 12 $

Medium:

MS IE Information Disclosure and Web Site Spoofing Vulnerabilities
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:803305
Summary:
This host is installed with Microsoft Internet Explorer and is
prone to information disclosure and web site spoofing vulnerabilities.
Vulnerability Insight:
The proxy settings configuration has same proxy address and value for HTTP
and HTTPS,
- TCP session to proxy sever will not properly be reused. This allows remote
attackers to steal cookie information via crafted HTML document.
- SSl lock consistency with address bar is not ensured. This allows remote
attackers to spoof web sites via a crafted HTML document.
Impact:
Successful exploitation allows attackers to disclose the
sensitive information and view the contents of spoofed site or carry out
phishing attacks.
Impact Level: Application
Affected Software/OS:
Microsoft Internet Explorer versions 8 and 9
Solution:
No solution or patch was made available for at least one year
since disclosure of this vulnerability. Likely none will be provided anymore.
General solution options are to upgrade to a newer release, disable respective
features, remove the product or replace the product by another one.
CVSS Base Score : 4.0
Family name: Windows
Category: infos
Copyright: Copyright (c) 2013 Greenbone Networks GmbH
Summary: Check the vulnerable version of Microsoft Internet Explorer
Version: $Revision: 346 $

Medium:

Microsoft Windows Group Policy Security Feature Bypass Vulnerability (3004361)
Risk:Medium
Application:general
Port:0
Protocol:tcp
ScriptID:805273
NODESC
CVSS Base Score : 3.3
Family name: Windows : Microsoft Bulletins
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 1015 $

Low:

SMB Test
Risk:Low
Application:general
Port:0
Protocol:SMBCl
ScriptID:90011
OS Version = WINDOWS SERVER (R) 2008 STANDARD 6002 SERVICE PACK 2
Domain = WORKGROUP
SMB Serverversion = WINDOWS SERVER (R) 2008 STANDARD 6.0
CVSS Base Score : 0.0
Family name: Windows
Category: infos
Copyright: Copyright (C) 2008 Greenbone Networks GmbH
Summary: Determines the OS and SMB Version of Host
Version: $Revision: 16 $

Low:

Windows SharePoint Services detection
Risk:Low
Application:http
Port:80
Protocol:tcp
ScriptID:101018
Server: Microsoft-IIS/7.0
Operating System Type: Windows 2008 / Vista
CVSS Base Score : 0.0
Family name: Service detection
Category: infos
Copyright: Christian Eric Edjenguele <christian.edjenguele@owasp.org>
Summary: Windows SharePoint Services Information Gathering
Version: $Revision: 43 $

Low:

SMB Enumerate Services
Risk:Low
Application:microsoft-ds
Port:445
Protocol:tcp
ScriptID:102016
WIN32 active services:
Application Experience [AeLookupSvc]
Application Host Helper Service [AppHostSvc]
Base Filtering Engine [BFE]
Background Intelligent Transfer Service [BITS]
Certificate Propagation [CertPropSvc]
COM+ System Application [COMSysApp]
Cryptographic Services [CryptSvc]
DCOM Server Process Launcher [DcomLaunch]
DHCP Client [Dhcp]
DNS Client [Dnscache]
Diagnostic Policy Service [DPS]
Windows Event Log [EventLog]
COM+ Event System [EventSystem]
Group Policy Client [gpsvc]
IKE and AuthIP IPsec Keying Modules [IKEEXT]
IP Helper [iphlpsvc]
KtmRm for Distributed Transaction Coordinator [KtmRm]
Server [LanmanServer]
Workstation [LanmanWorkstation]
Distributed Transaction Coordinator [MSDTC]
Network Connections [Netman]
Network List Service [netprofm]
Network Location Awareness [NlaSvc]
Network Store Interface Service [nsi]
Plug and Play [PlugPlay]
IPsec Policy Agent [PolicyAgent]
User Profile Service [ProfSvc]
Remote Registry [RemoteRegistry]
Remote Procedure Call (RPC) [RpcSs]
Security Accounts Manager [SamSs]
Task Scheduler [Schedule]
Secondary Logon [seclogon]
System Event Notification Service [SENS]
Terminal Services Configuration [SessionEnv]
Shell Hardware Detection [ShellHWDetection]
Software Licensing [slsvc]
Print Spooler [Spooler]
Secure Socket Tunneling Protocol Service [SstpSvc]
Terminal Services [TermService]
Distributed Link Tracking Client [TrkWks]
Terminal Services UserMode Port Redirector [UmRdpService]
Desktop Window Manager Session Manager [UxSms]
VMware Tools [VMTools]
World Wide Web Publishing Service [W3SVC]

Windows Process Activation Service [WAS]
Diagnostic System Host [WdiSystemHost]
Windows Error Reporting Service [WerSvc]
Windows Management Instrumentation [Winmgmt]
Windows Remote Management (WS-Management) [WinRM]
winexesvc [winexesvc]
##
WIN32 inactive services:
Application Layer Gateway Service [ALG]
Application Information [Appinfo]
Application Management [AppMgmt]
Windows Audio Endpoint Builder [AudioEndpointBuilder]
Windows Audio [Audiosrv]
Computer Browser [Browser]
Microsoft .NET Framework NGEN v2.0.50727_X86 [clr_optimization_v2.0.50727_32]
Offline Files [CscService]
Wired AutoConfig [dot3svc]
Extensible Authentication Protocol [EapHost]
Microsoft Fibre Channel Platform Registration Service [FCRegSvc]
Function Discovery Provider Host [fdPHost]
Function Discovery Resource Publication [FDResPub]
Windows Font Cache Service [FontCache]
Windows Presentation Foundation Font Cache 3.0.0.0 [FontCache3.0.0.0]
Human Interface Device Access [hidserv]
Health Key and Certificate Management [hkmsvc]
Windows CardSpace [idsvc]
PnP-X IP Bus Enumerator [IPBusEnum]
CNG Key Isolation [KeyIso]
Link-Layer Topology Discovery Mapper [lltdsvc]
TCP/IP NetBIOS Helper [lmhosts]
Multimedia Class Scheduler [MMCSS]
Mozilla Maintenance Service [MozillaMaintenance]
Windows Firewall [MpsSvc]
Microsoft iSCSI Initiator Service [MSiSCSI]
Windows Installer [msiserver]
Network Access Protection Agent [napagent]
Netlogon [Netlogon]
Net.Tcp Port Sharing Service [NetTcpPortSharing]
Performance Logs & Alerts [pla]
Protected Storage [ProtectedStorage]
Remote Access Auto Connection Manager [RasAuto]
Remote Access Connection Manager [RasMan]
Routing and Remote Access [RemoteAccess]
Remote Procedure Call (RPC) Locator [RpcLocator]
Resultant Set of Policy Provider [RSoPProv]
Special Administration Console Helper [sacsvr]
Smart Card [SCardSvr]
Smart Card Removal Policy [SCPolicySvc]
Internet Connection Sharing (ICS) [SharedAccess]
SL UI Notification Service [SLUINotify]
SNMP Trap [SNMPTRAP]
SSDP Discovery [SSDPSRV]
Microsoft Software Shadow Copy Provider [swprv]

Superfetch [SysMain]
Telephony [TapiSrv]
TPM Base Services [TBS]
Themes [Themes]
Thread Ordering Server [THREADORDER]
Windows Modules Installer [TrustedInstaller]
Interactive Services Detection [UI0Detect]
UPnP Device Host [upnphost]
Virtual Disk [vds]
VMware Snapshot Provider [vmvss]
Volume Shadow Copy [VSS]
Windows Time [W32Time]
Windows Color System [WcsPlugInService]
Diagnostic Service Host [WdiServiceHost]
Windows Event Collector [Wecsvc]
Problem Reports and Solutions Control Panel Support [wercplsupport]
WinHTTP Web Proxy Auto-Discovery Service [WinHttpAutoProxySvc]
WMI Performance Adapter [wmiApSrv]
Portable Device Enumerator Service [WPDBusEnum]
Windows Update [wuauserv]
Windows Driver Foundation - User-mode Driver Framework [wudfsvc]
OSSEC HIDS [OssecSvc]
##
WIN32 active drivers:
Microsoft ACPI Driver [ACPI]
Ancilliary Function Driver for Winsock [AFD]
Intel AGP Bus Filter [agp440]
RAS Asynchronous Media Driver [AsyncMac]
IDE Channel [atapi]
Beep [Beep]
bowser [bowser]
CD/DVD File System Reader [cdfs]
CD-ROM Driver [cdrom]
Common Log (CLFS) [CLFS]
Microsoft AC Adapter Driver [CmBatt]
Microsoft Composite Battery Driver [Compbatt]
Crcdisk Filter Driver [crcdisk]
DFS Namespace Client Driver [DfsC]
Disk Driver [disk]
LDDM Graphics Subsystem [DXGKrnl]
Intel(R) PRO/1000 NDIS 6 Adapter Driver [E1G60]
FltMgr [FltMgr]
HTTP [HTTP]
i8042 Keyboard and PS/2 Mouse Port Driver [i8042prt]
intelide [intelide]
Intel Processor Driver [intelppm]
iScsiPort Driver [iScsiPrt]
Keyboard Class Driver [kbdclass]
KSecDD [KSecDD]
Sync Driver [LGTO_Sync]
Link-Layer Topology Discovery Mapper I/O Driver [lltdio]
LSI_SCSI [LSI_SCSI]
UAC File Virtualization [luafv]

Microsoft Monitor Class Function Driver Service [monitor]
Mouse Class Driver [mouclass]
Mount Point Manager [mountmgr]
SMB MiniRedirector Wrapper and Engine [mrxsmb]
SMB 1.x MiniRedirector [mrxsmb10]
SMB 2.0 MiniRedirector [mrxsmb20]
Msfs [Msfs]
ISA/EISA Class Driver [msisadrv]
Microsoft System Management BIOS Driver [mssmbios]
Mup [Mup]
NDIS System Driver [NDIS]
Remote Access NDIS TAPI Driver [NdisTapi]
Remote Access NDIS WAN Driver [NdisWan]
NDIS Proxy [NDProxy]
NetBIOS Interface [NetBIOS]
NetBT [NetBT]
Npfs [Npfs]
NSI proxy service [nsiproxy]
Ntfs [Ntfs]
Null [Null]
Parallel port driver [Parport]
Partition Manager [partmgr]
Parvdm [Parvdm]
PCI Bus Driver [pci]
PEAUTH [PEAUTH]
WAN Miniport (PPTP) [PptpMiniport]
QoS Packet Scheduler [PSched]
Remote Access Auto Connection Driver [RasAcd]
WAN Miniport (L2TP) [Rasl2tp]
Remote Access PPPOE Driver [RasPppoe]
WAN Miniport (SSTP) [RasSstp]
Redirected Buffering Sub Sysytem [rdbss]
RDPCDD [RDPCDD]
Terminal Server Device Redirector Driver [rdpdr]
RDP Encoder Mirror Driver [RDPENCDD]
RDP Winstation Driver [RDPWD]
Link-Layer Topology Discovery Responder [rspndr]
##
CVSS Base Score : 0.0
Family name: Windows
Category: infos
Copyright: Copyright(C) 2010 LSS
Summary: Enumerates the list of remote services and drivers
Version: $Revision: 44 $

Low:

CPE Inventory
Risk:Low
Application:general
Port:0
Protocol:CPE-T
ScriptID:810002
10.47.30.102|cpe:/a:microsoft:ie:8.0.6001.18999
10.47.30.102|cpe:/a:microsoft:iis:7.0
10.47.30.102|cpe:/a:microsoft:windows_media_player:0
10.47.30.102|cpe:/a:mozilla:firefox:37.0.1
10.47.30.102|cpe:/o:microsoft:windows_server_2008::sp2
CVSS Base Score : 0.0
Family name: Service detection
Category: end
Copyright: Copyright (c) 2009 Greenbone Networks GmbH
Summary: CPE Inventory
Version: $Revision: 314 $

Low:

Host Summary
Risk:Low
Application:general
Port:0
Protocol:HOST-
ScriptID:810003
traceroute:10.47.30.100,10.47.30.102
TCP ports:80,445,135,3389
UDP ports:
CVSS Base Score : 0.0
Family name: General
Category: end
Copyright: Copyright (c) 2010 Greenbone Networks GmbH
Summary: Host Summary
Version: $Revision: 14 $

Low:

ICMP Timestamp Detection
Risk:Low
Application:general
Port:0
Protocol:icmp
ScriptID:103190
Summary:
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.
CVSS Base Score : 0.0
Family name: Service detection
Category: infos
Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH
Summary: Checks if the remote host answers to ICMP Timestamp requests
Version: $Revision: 13 $

Low:

OS fingerprinting
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:102002
ICMP based OS fingerprint results: (95% confidence)
Microsoft Windows
CVSS Base Score : 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2009 LSS
Summary: Detects remote operating system version
Version: $Revision: 43 $

Low:

DIRB (NASL wrapper)
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:103079
DIRB could not be found in your system path.
OpenVAS was unable to execute DIRB and to perform the scan you
requested.
Please make sure that DIRB is installed and is
available in the PATH variable defined for your environment.
CVSS Base Score : 0.0
Family name: Web application abuses
Category: infos
Copyright: Copyright (C) 2011 Greenbone Networks GmbH
Summary: Brute force web app directories/files
Version: $Revision: 13 $

Low:

Checks for open udp ports
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:103978
Open UDP ports: [None found]
CVSS Base Score : 0.0
Family name: General
Category: infos
Copyright: Copyright (c) 2012 Greenbone Networks GmbH
Summary: Check Open UDP Ports
Version: $Revision: 357 $

Low:

SMB Registry : Windows Service Pack version
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:10401
The Windows Server (R) 2008 Standard 6.0 is installed with Service Pack 2
CVSS Base Score : 0.0
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2000 Renaud Deraison
Summary: Check for Service Pack on the remote host
Version: $Revision: 549 $

Low:

arachni (NASL wrapper)
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:110001
Arachni could not be found in your system path.
OpenVAS was unable to execute Arachni and to perform the scan you
requested.
Please make sure that Arachni is installed and that arachni is
available in the PATH variable defined for your environment.
CVSS Base Score : 0.0
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2011 Michelangelo Sidagni
Summary: Assess web security with arachni
Version: $Revision: 683 $

Low:

Netstat 'scanner'
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:14272
No port for an ssh connect was found open.
Hence not able to run netstat command.
CVSS Base Score : 0.0
Family name: Port scanners
Category: scanner
Copyright: This script is Copyright (C) 2004 Michel Arboi
Summary: Find open ports with netstat
Version: $Revision: 1101 $

Low:

Traceroute
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:51662
Here is the route from 10.47.30.100 to 10.47.30.102:
10.47.30.100
10.47.30.102
CVSS Base Score : 0.0
Family name: General
Category: infos
Copyright: Copyright (c) 2005 E-Soft Inc. http://www.securityspace.com
Summary: Traceroute
Version: $Revision: 975 $

Low:

Mozilla Firefox Version Detection (Windows)
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:800014
Detected Mozilla Firefox
Version: 37.0.1
Location: C:\Program Files\Mozilla Firefox
CPE: cpe:/a:mozilla:firefox:37.0.1
Concluded from version identification result:
37.0.1
CVSS Base Score : 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2008 Greenbone Networks GmbH
Summary: Detection of installed version of Mozilla Firefox
Version: $Revision: 904 $

Low:

Mozilla Firefox Version Detection (Windows)
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:800014
Detected Mozilla Firefox
Version: 37.0.1 (x86 en-US)
Location: C:\Program Files\Mozilla Firefox
CPE: cpe:/a:mozilla:firefox:37.0.1
Concluded from version identification result:
37.0.1 (x86 en-US)
CVSS Base Score : 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2008 Greenbone Networks GmbH
Summary: Detection of installed version of Mozilla Firefox
Version: $Revision: 904 $

Low:

Microsoft Internet Explorer Version Detection (Win)
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:800209
Detected Microsoft Internet Explorer
Version: 8.0.6001.18999
Location: C:\Program Files\Internet Explorer
CPE: cpe:/a:microsoft:ie:8.0.6001.18999
Concluded from version identification result:
8.0.6001.18999
CVSS Base Score : 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (C) 2008 Greenbone Networks GmbH
Summary: Check for Internet Explorer version
Version: $Revision: 42 $

Low:

Microsoft Internet Information Services (IIS) Version Detection
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:802432
Detected Microsoft Internet Information Services
Version: 7.0
Location: %windir%\system32\inetsrv
CPE: cpe:/a:microsoft:iis:7.0
Concluded from version identification result:
7.0
CVSS Base Score : 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2012 Greenbone Networks GmbH
Summary: Set the Version of Internet Information Services (IIS) in KB
Version: $Revision: 44 $

Low:

Compatibility Issues Affecting Signed Microsoft Binaries (2749655)
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:802468
Summary:
The host is installed with Microsoft Windows operating system and
its missing upates according to Microsoft Security Advisory (2749655)
Vulnerability Insight:
Issue involving binaries that were signed with digital certificates generated
by Microsoft without proper timestamp attributes. This issue is caused by a
missing timestamp Enhanced Key Usage (EKU) extension during certificate
generation and signing of Microsoft core components and software.
Impact:
This could cause compatibility issues between affected binaries and
Microsoft Windows and This issue could adversely impact the ability to properly
install and uninstall affected Microsoft components and security updates.
Impact Level: System
Affected Software/OS:
Microsoft Windows XP x32 Edition Service Pack 3 and prior
Microsoft Windows XP x64 Edition Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
Solution:
Apply the Patch from below link,
http://technet.microsoft.com/en-us/security/advisory/2749655
CVSS Base Score : 0.0
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH
Summary: Check for the vulnerable Wintrust.dll file version
Version: $Revision: 12 $

Low:

Microsoft SMB Signing Disabled
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:802726
SMB signing is disabled on this host
CVSS Base Score : 0.0
Family name: Windows
Category: infos
Copyright: Copyright (c) 2012 Greenbone Networks GmbH
Summary: Check if SMB signing is disabled
Version: $Revision: 12 $

Low:

Microsoft Windows Media Player Version Detection
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:900173
Detected Microsoft Windows Media Player
Version: 0
Location: Could not find the install location from registry
CPE: cpe:/a:microsoft:windows_media_player:0
Concluded from version identification result:
0
CVSS Base Score : 0.0
Family name: General
Category: infos
Copyright: Copyright (C) 2008 SecPod
Summary: Set File Version of Windows Media Player in KB
Version: $Revision: 575 $

Low:

Checks for open tcp ports
Risk:Low
Application:general
Port:0
Protocol:tcp
ScriptID:900239
Open TCP ports: 80, 445, 135, 3389
CVSS Base Score : 0.0
Family name: General
Category: infos
Copyright: Copyright (C) 2010 SecPod
Summary: Check Open TCP Ports
Version: $Revision: 357 $

Low:

HTTP Server type and version
Risk:Low
Application:http
Port:80
Protocol:tcp
ScriptID:10107
The remote web server type is :
Microsoft-IIS/7.0
CVSS Base Score : 0.0
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2000 H. Scholz & Contributors
Summary: HTTP Server type and version
Version: $Revision: 229 $

Low:

Services
Risk:Low
Application:http
Port:80
Protocol:tcp
ScriptID:10330
A web server is running on this port
CVSS Base Score : 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: Find what is listening on which port
Version: $Revision: 69 $

Low:

Nikto (NASL wrapper)
Risk:Low
Application:http
Port:80
Protocol:tcp
ScriptID:14260
Here is the Nikto report:
Unknown option: ask
-Cgidirs+ scan these CGI dirs: 'none', 'all', or values like "/cgi/ /cgi-a/"
-dbcheck check database and other key files for syntax errors (cannot be abbreviated)
-evasion+ ids evasion technique
-Format+ save file (-o) format
-host+ target host
-Help Extended help information
-id+ host authentication to use, format is userid:password
-list-plugins List all available plugins
-mutate+ Guess additional file names
-mutate-options+ Provide extra information for mutations
-output+ Write output to this file
-nocache Disables the URI cache
-nossl Disables using SSL
-no404 Disables 404 checks
-Plugins List of plugins to run (default ALL)
-port+ Port to use (default 80)
-Display+ Turn on/off display outputs
-ssl Force ssl mode on port
-Single Single request mode
-timeout+ Timeout (default 2 seconds)
-Tuning+ Scan tuning
-update Update databases and plugins from cirt.net (cannot be abbreviated)
-Version Print plugin and database versions
-vhost+ Virtual host (for Host header)
+ requires a value
CVSS Base Score : 0.0
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2004 Michel Arboi
Summary: Assess web server security with Nikto
Version: $Revision: 995 $

Low:

wapiti (NASL wrapper)
Risk:Low
Application:http
Port:80
Protocol:tcp
ScriptID:80110
wapiti could not be found in your system path.
OpenVAS was unable to execute wapiti and to perform the scan you
requested.
Please make sure that wapiti is installed and that wapiti is
available in the PATH variable defined for your environment.
CVSS Base Score : 0.0
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2010 Vlatko Kosturjak
Summary: Assess web security with wapiti
Version: $Revision: 14 $

Low:

Microsoft IIS Webserver Version Detection
Risk:Low
Application:http
Port:80
Protocol:tcp
ScriptID:900710
Detected Microsoft IIS Webserver
Version: 7.0
Location: 80/tcp
CPE: cpe:/a:microsoft:iis:7.0
Concluded from version identification result:
IIS/7.0
CVSS Base Score : 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (C) 2009 SecPod
Summary: Set the Version of Microsoft IIS in KB
Version: $Revision: 43 $

Low:

SMB NativeLanMan
Risk:Low
Application:microsoft-ds
Port:445
Protocol:tcp
ScriptID:102011
Summary:
It is possible to extract OS, domain and SMB server information
from the Session Setup AndX Response packet which is generated
during NTLM authentication.Detected SMB workgroup: WORKGROUP
Detected SMB server: Windows Server (R) 2008 Standard 6.0
Detected OS: Windows Server (R) 2008 Standard 6002 Service Pack 2
CVSS Base Score : 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (C) 2009 LSS
Summary: Extracts info about the OS through NTLM authentication packets
Version: $Revision: 43 $

Low:

SMB log in
Risk:Low
Application:microsoft-ds
Port:445
Protocol:tcp
ScriptID:10394
It was possible to log into the remote host using the SMB protocol.
CVSS Base Score : 0.0
Family name: Windows
Category: infos
Copyright: Copyright (C) 2008 SecPod
Summary: Attempts to log into the remote host
Version: $Revision: 1032 $

Low:

SMB on port 445
Risk:Low
Application:microsoft-ds
Port:445
Protocol:tcp
ScriptID:11011
A CIFS server is running on this port
CVSS Base Score : 0.0
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2002 Renaud Deraison
Summary: Checks for openness of port 445
Version: $Revision: 41 $

Low:

Microsoft Windows SMB Accessible Shares
Risk:Low
Application:microsoft-ds
Port:445
Protocol:tcp
ScriptID:902425
The following shares where found
C$
ADMIN$
IPC$
E$
CVSS Base Score : 0.0
Family name: Windows
Category: infos
Copyright: Copyright (c) 2012 SecPod
Summary: Check for SMB Accessible Shares
Version: $Revision: 977 $

Low:

Services
Risk:Low
Application:ms-wbt-server
Port:3389
Protocol:tcp
ScriptID:10330
A TLSv1 server answered on this port
CVSS Base Score : 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: Find what is listening on which port
Version: $Revision: 69 $

Low:

Check for supported SSL Ciphers
Risk:Low
Application:ms-wbt-server
Port:3389
Protocol:tcp
ScriptID:103441
Service does not support SSLv2 Ciphers.
Service does not support SSLv3 Ciphers.
Service does not support TLSv1 Ciphers.
No medium ciphers are supported by this service
No weak ciphers are supported by this service
No non-ciphers are supported by this service
CVSS Base Score : 0.0
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH
Summary: Checks for supported SSL Weak
Version: $Revision: 12 $

Low:

SSL Certificate Expiry
Risk:Low
Application:ms-wbt-server
Port:3389
Protocol:tcp
ScriptID:15901
The SSL certificate of the remote service is valid between
2015-06-09 19:13:13 GMT and 2015-12-09 19:13:13 GMT.
CVSS Base Score : 0.0
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2004 George A. Theall
Summary: Checks SSL certificate expiry
Version: $Revision: 989 $

Low:

Identify unknown services with nmap
Risk:Low
Application:ms-wbt-server
Port:3389
Protocol:tcp
ScriptID:66286
Nmap service detection result for this port: ms-wbt-server
CVSS Base Score : 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (c) 2009 E-Soft Inc. http://www.securityspace.com
Summary: Launches nmap -sV against ports running unidentified services
Version: $Revision: 329 $

Low:

Check for SSL Ciphers
Risk:Low
Application:ms-wbt-server
Port:3389
Protocol:tcp
ScriptID:802067
Service does not support SSLv2 Ciphers.
Service does not support SSLv3 Ciphers.
Service does not support TLSv1 Ciphers.
No medium ciphers are supported by this service
No weak ciphers are supported by this service
No non-ciphers are supported by this service
CVSS Base Score : 0.0
Family name: General
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: Checks for the SSL Ciphers
Version: $Revision: 312 $

Info:

Risk:Info
Application:epmap
Port:135
Protocol:tcp
ScriptID:0
Open port.
CVSS Base Score : -

Info:

Risk:Info
Application:http
Port:80
Protocol:tcp
ScriptID:0
Open port.
CVSS Base Score : -

Info:

Risk:Info
Application:microsoft-ds
Port:445
Protocol:tcp
ScriptID:0
Open port.
CVSS Base Score : -

Info:

Risk:Info
Application:ms-wbt-server
Port:3389
Protocol:tcp
ScriptID:0
Open port.
CVSS Base Score : -