TENABLE NETWORK SECURITY, INC.

WSUS Monitoring Report

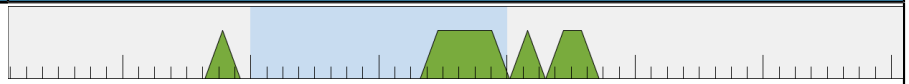
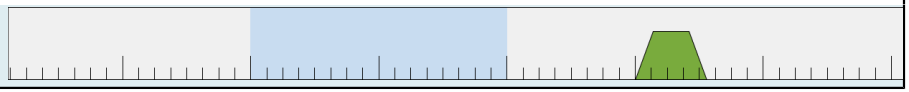
August 30, 2012 at 2:24am CDT
Dave Breslin [dbreslin]

TENABLE
Network Security®

Table of Contents

WSUS Server and Client Event Counts (Past 7 Days)

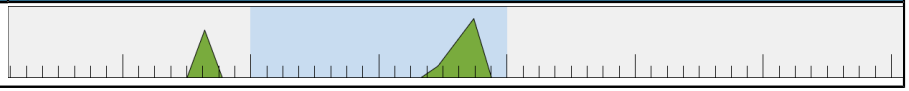
WSUS Server Events

Event	Count	Aug 23, 2012 02:24:36 to Aug 30, 2012 02:24:36
WSUS-High_Update_Error_Rate	8	
WSUS-Missing_Clients	3	

WSUS Client Events - Windows Update Successful

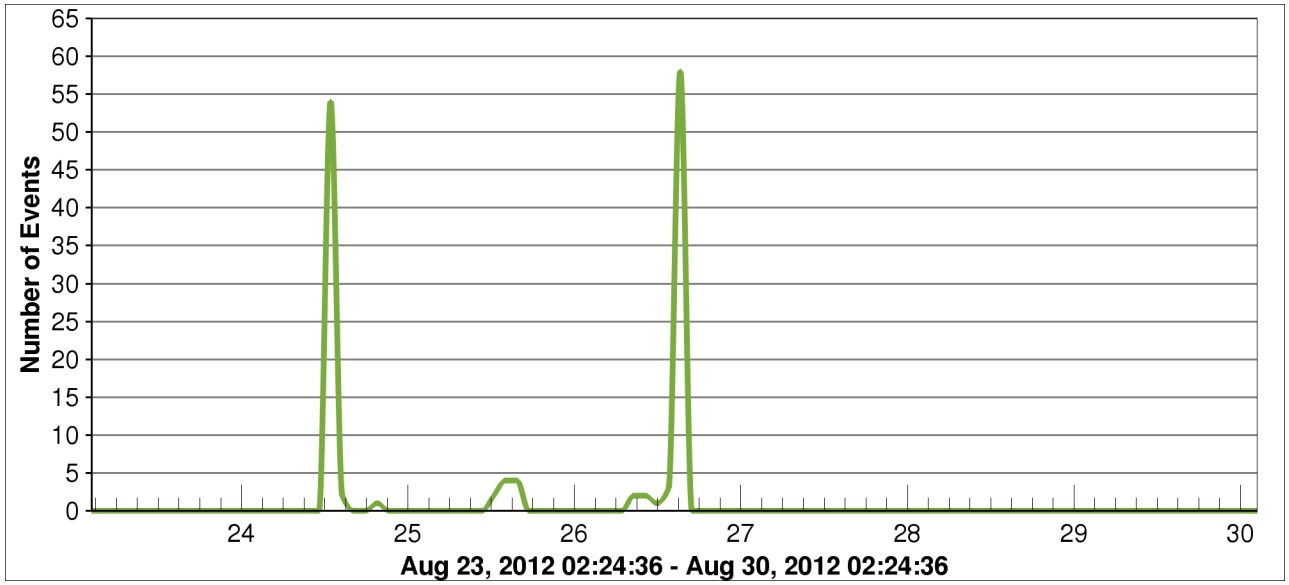
Event	Count	Aug 23, 2012 02:24:36 to Aug 30, 2012 02:24:36
Windows-Update_Successful	133	

WSUS Client Events - Windows Update Install Failed

Event	Count	Aug 23, 2012 02:24:36 to Aug 30, 2012 02:24:36
Windows-UpdateClient_Installation_Failure	13	

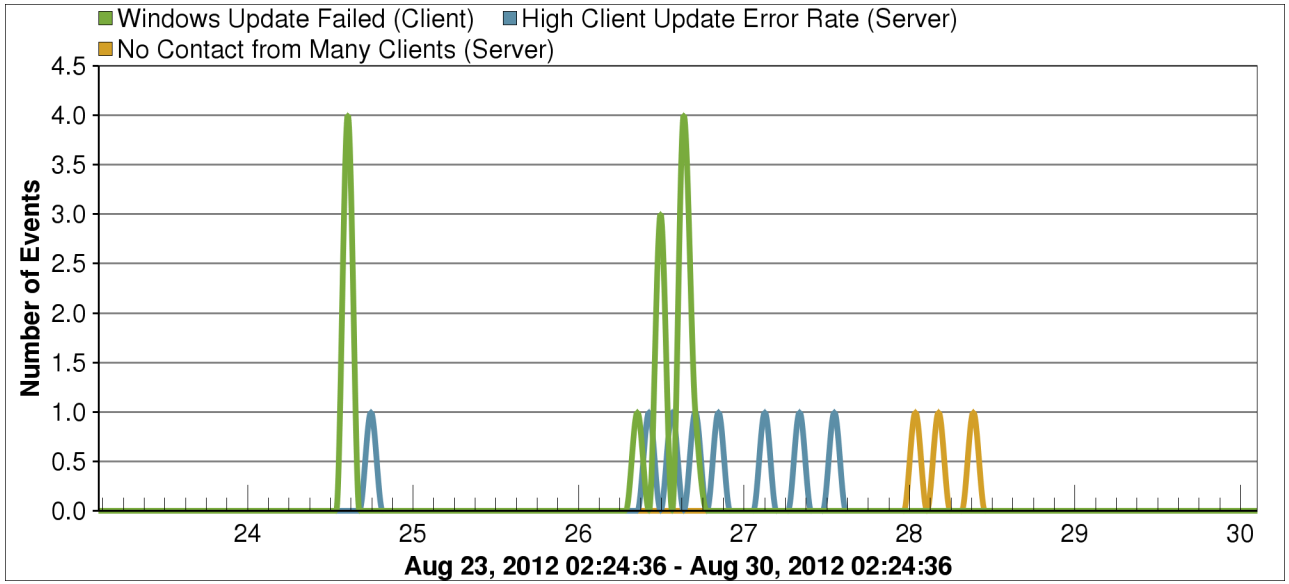
WSUS Clients - Windows Update Successful Events (Past 7 Days)

WSUS Clients - Windows Update Successful Events



WSUS Server and Client Failure Events (Past 7 Days)

WSUS Failure Events



WSUS Server Failure Events

Time	Sensor	Message
Aug 24, 2012 17:56:18 CDT	WSUS-SERV1	Application,08/24/2012,17:56:05 PM,Windows Server Update Services,13001,Warning,None,N/A,WSUS-SERV1,IP:10.0.0.71,13001,Client computers are installing updates with a higher than 10 percent failure rate. This should be monitored.
Aug 26, 2012 09:30:37 CDT	WSUS-SERV1	Application,08/26/2012,09:30:11 AM,Windows Server Update Services,13001,Warning,None,N/A,WSUS-SERV1,IP:10.0.0.71,13001,Client computers are installing updates with a higher than 10 percent failure rate. This should be monitored.
Aug 26, 2012 14:10:37 CDT	WSUS-SERV1	Application,08/26/2012,14:10:13 PM,Windows Server Update Services,13001,Warning,None,N/A,WSUS-SERV1,IP:10.0.0.71,13001,Client computers are installing updates with a higher than 10 percent failure rate. This should be monitored.
Aug 26, 2012 16:50:37 CDT	WSUS-SERV1	Application,08/26/2012,16:50:15 PM,Windows Server Update Services,13001,Warning,None,N/A,WSUS-SERV1,IP:10.0.0.71,13001,Client computers are installing updates with a higher than 10 percent failure rate. This should be monitored.
Aug 26, 2012 20:11:04 CDT	WSUS-SERV1	Application,08/26/2012,20:10:16 PM,Windows Server Update Services,13001,Warning,None,N/A,WSUS-SERV1,IP:10.0.0.71,13001,Client computers are installing updates with a higher than 10 percent failure rate. This should be monitored.
Aug 27, 2012 02:11:04 CDT	WSUS-SERV1	Application,08/27/2012,02:10:24 AM,Windows Server Update Services,13001,Warning,None,N/A,WSUS-SERV1,IP:10.0.0.71,13001,Client computers are installing updates with a higher than 10 percent failure rate. This should be monitored.
Aug 27, 2012 08:11:04 CDT	WSUS-SERV1	Application,08/27/2012,08:10:27 AM,Windows Server Update Services,13001,Warning,None,N/A,WSUS-SERV1,IP:10.0.0.71,13001,Client computers are installing updates with a higher than 10 percent failure rate. This should be monitored.
Aug 27, 2012 13:11:53 CDT	WSUS-SERV1	Application,08/27/2012,13:11:08 PM,Windows Server Update Services,13001,Warning,None,N/A,WSUS-SERV1,IP:10.0.0.71,13001,Client computers are installing updates with a higher than 10 percent failure rate. This should be monitored.
Aug 28, 2012 00:06:51 CDT	WSUS-SERV1	Application,08/28/2012,00:06:07 AM,Windows Server Update Services,13032,Error,None,N/A,WSUS-SERV1,IP:10.0.0.71,13032,Many client computers have not reported back to the server in the last 1 days. 6 have been detected so far.

Time	Sensor	Message
Aug 28, 2012 03:56:51 CDT	WSUS-SERV1	Application,08/28/2012,03:56:09 AM,Windows Server Update Services,13032,Error,None,N/A,WSUS-SERV1,IP:10.0.0.71,13032,Many client computers have not reported back to the server in the last 1 days. 6 have been detected so far.
Aug 28, 2012 09:56:51 CDT	WSUS-SERV1	Application,08/28/2012,09:56:12 AM,Windows Server Update Services,13032,Error,None,N/A,WSUS-SERV1,IP:10.0.0.71,13032,Many client computers have not reported back to the server in the last 1 days. 6 have been detected so far.

WSUS Client Update Installation Failure Events by Location

	Count
HQ 2nd Floor	26
HQ 1st Floor	0
HQ 3rd Floor	0
Distribution Center 1	0
Distribution Center 2	0
Distribution Center 3	0
Distribution Center 4	0
HQ Wireless	0
HQ Mgmt	0

10.0.0.122

IP Address: 10.0.0.122
DNS Name: dt0006-pc.itsdept.com
MAC Address: 08:00:27:ec:ad:a8
NetBIOS Name: ITSDEPT\DT0006-PC

Details

Time	Sensor	Message
Aug 24, 2012 13:50:09 CDT	DT0006-PC	System,08/24/2012,13:50:00 PM,Microsoft-Windows-WindowsUpdateClient,20,Error,Installation,Windows Update Agent,N/A,DT0006-PC,IP:10.0.0.122,20,Installation Failure: Windows failed to install the following update with error 0x800b0100: Update for Windows 7 for x64-based Systems (KB2533552).
Aug 24, 2012 13:54:09 CDT	DT0006-PC	System,08/24/2012,13:53:26 PM,Microsoft-Windows-WindowsUpdateClient,20,Error,Installation,Windows Update Agent,N/A,DT0006-PC,IP:10.0.0.122,20,Installation Failure: Windows failed to install the following update with error 0x80073715: Update for Windows 7 for x64-based Systems (KB2533552).
Aug 24, 2012 14:00:39 CDT	DT0006-PC	System,08/24/2012,13:59:53 PM,Microsoft-Windows-WindowsUpdateClient,20,Error,Installation,Windows Update Agent,N/A,DT0006-PC,IP:10.0.0.122,20,Installation Failure: Windows failed to install the following update with error 0x80070002: Update for Windows 7 for x64-based Systems (KB2533552).
Aug 24, 2012 14:00:39 CDT	DT0006-PC	System,08/24/2012,14:00:22 PM,Microsoft-Windows-WindowsUpdateClient,20,Error,Installation,Windows Update Agent,N/A,DT0006-PC,IP:10.0.0.122,20,Installation Failure: Windows failed to install the following update with error 0x80070002: Update for Windows 7 for x64-based Systems (KB2533552).
Aug 26, 2012 16:52:33 CDT	DT0006-PC	System,08/26/2012,16:52:02 PM,Microsoft-Windows-WindowsUpdateClient,20,Error,Installation,Windows Update Agent,N/A,DT0006-PC,IP:10.0.0.122,20,Installation Failure: Windows failed to install the following update with error 0x8024d00e: Windows Update Core.

10.0.0.115

IP Address: 10.0.0.115
DNS Name: dt0003-pc.itsdept.com
MAC Address: 08:00:27:6a:c0:95
NetBIOS Name: ITSDEPT\DT0003-PC

Details

Time	Sensor	Message
Aug 26, 2012 14:55:49 CDT	DT0003-PC	System,08/26/2012,14:55:50 PM,Microsoft-Windows-WindowsUpdateClient,20,Error,Installation,Windows Update Agent,N/A,DT0003-PC,IP:10.0.0.115,20,Installation Failure: Windows failed to install the following update with error 0x80073712: Security Update for Windows 7 for x64-based Systems (KB2644615).
Aug 26, 2012 14:55:49 CDT	DT0003-PC	System,08/26/2012,14:55:50 PM,Microsoft-Windows-WindowsUpdateClient,20,Error,Installation,Windows Update Agent,N/A,DT0003-PC,IP:10.0.0.115,20,Installation Failure: Windows failed to install the following update with error 0x800b0100: Security Update for Windows 7 for x64-based Systems (KB2698365).
Aug 26, 2012 14:57:49 CDT	DT0003-PC	System,08/26/2012,14:57:23 PM,Microsoft-Windows-WindowsUpdateClient,20,Error,Installation,Windows Update Agent,N/A,DT0003-PC,IP:10.0.0.115,20,Installation Failure: Windows failed to install the following update with error 0x800b0100: Cumulative Security Update for Internet Explorer 8 for Windows 7 for x64-based Systems (KB2722913).
Aug 26, 2012 15:13:49 CDT	DT0003-PC	System,08/26/2012,15:13:16 PM,Microsoft-Windows-WindowsUpdateClient,20,Error,Installation,Windows Update Agent,N/A,DT0003-PC,IP:10.0.0.115,20,Installation Failure: Windows failed to install the following update with error 0x80073715: Security Update for Internet Explorer 8 for Windows 7 for x64-based Systems (KB2544521).

10.0.0.114

IP Address: 10.0.0.114
DNS Name: dt0002-pc.itsdept.com
MAC Address: 08:00:27:c8:f7:c3
NetBIOS Name: ITSDEPT\DT0002-PC

Details

Time	Sensor	Message
Aug 26, 2012 12:23:26 CDT	DT0002-PC	System,08/26/2012,12:23:13 PM,Microsoft-Windows-WindowsUpdateClient,20,Error,Installation,Windows Update Agent,N/A,DT0002-PC,IP:10.0.0.114,20,Installation Failure: Windows failed to install the following update with error 0x80073712: Security Update for Windows 7 for x64-based Systems (KB2584146).
Aug 26, 2012 12:23:26 CDT	DT0002-PC	System,08/26/2012,12:23:23 PM,Microsoft-Windows-WindowsUpdateClient,20,Error,Installation,Windows Update Agent,N/A,DT0002-PC,IP:10.0.0.114,20,Installation Failure: Windows failed to install the following update with error 0x80073712: Security Update for Windows 7 for x64-based Systems (KB2644615).
Aug 26, 2012 12:23:26 CDT	DT0002-PC	System,08/26/2012,12:23:23 PM,Microsoft-Windows-WindowsUpdateClient,20,Error,Installation,Windows Update Agent,N/A,DT0002-PC,IP:10.0.0.114,20,Installation Failure: Windows failed to install the following update with error 0x800b0100: Security Update for Windows 7 for x64-based Systems (KB2698365).

10.0.0.113

IP Address: 10.0.0.113
DNS Name: dt0001-pc.itsdept.com
MAC Address: 08:00:27:29:cd:93
NetBIOS Name: ITSDEPT\DT0001-PC

Details

Time	Sensor	Message
Aug 26, 2012 09:15:46 CDT	DT0001-PC	System,08/26/2012,09:15:23 AM,Microsoft-Windows-WindowsUpdateClient,20,Error,Installation,Windows Update Agent,N/A,DT0001-PC,IP:10.0.0.113,20,Installation Failure: Windows failed to install the following update with error 0x80073712: Security Update for Windows 7 for x64-based Systems (KB2584146).

Missing Security Updates with Known Exploits

Missing Security Updates

MS Bulletin	Total	Severity
MS12-054	3	Critical
MS12-008	3	High
MS12-009	3	High
MS12-020	3	High
MS12-023	3	High
MS12-034	3	High
MS12-037	3	High
MS12-038	3	High
MS12-042	3	High
MS12-043	3	High
MS12-004	2	High
MS12-005	2	High
MS12-019	3	Medium
MS12-049	3	Medium
MS12-006	2	Medium

Missing Security Updates Host Summary

IP Address	NetBIOS Name	DNS Name	MAC Address	Score	Repository	Total	Info	Low	Med.	High	Crit.
10.0.0.113	ITSDEPT\DT0001-PC	dt0001-pc.itsdept.com	08:00:27:29:cd:93	159	wsus	15	0	0	3	11	1
10.0.0.116	ITSDEPT\DT0004-PC	dt0004-pc.itsdept.com	08:00:27:68:c4:5b	136	wsus	12	0	0	2	9	1
10.0.0.122	ITSDEPT\DT0006-PC	dt0006-pc.itsdept.com	08:00:27:ec:ad:a8	159	wsus	15	0	0	3	11	1

10.0.0.122

NetBIOS Name: ITSDEPT\DT0006-PC
MAC Address: 08:00:27:ec:ad:a8
DNS Name: dt0006-pc.itsdept.com
Repository: wsus
Last Scan: Aug 30, 2012 @ 1:37AM

Details

Plugin	Plugin Name	Severity	Family	Exploit?
57472	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391)	High	Windows : Microsoft Bulletins	Yes

Synopsis: Opening a specially crafted media file could result in arbitrary code execution.

Description: The version of Windows Media installed on the remote host is affected by one or both of the following vulnerabilities :

- The Winmm.dll library as used by Windows Media Player does not properly handle specially crafted MIDI files. (CVE-2012-0003)

- A DirectShow component of DirectX does not properly handle specially crafted media files. (CVE-2012-0004)

An attacker who tricked a user on the affected host into opening a specially crafted MIDI or media file could leverage these issues to execute arbitrary code in the context of the current user.

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 as well as Windows XP Media Center Edition 2005 and Windows Media Center TV Pack 2008 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-004

Risk Factor: High

STIG Severity: II

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.7

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2631813 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-0003, CVE-2012-0004

BID: 51292, 51295

Crossref: OSVDB #78210, OSVDB #78211, EDB-ID #18426, MSFT #MS12-004, IAVA #2012-A-0005

Vulnerability Publication Date: 2012/01/10

Patch Publication Date: 2012/01/10

Plugin Publication Date: 2012/01/10

Plugin Modification Date: 2012/08/16

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-004.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks: Metasploit (MS12-004 midiOutPlayNextPolyEvent Heap Overflow)

Plugin	Plugin Name	Severity	Family	Exploit?
57473	MS12-005: Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146)	High	Windows : Microsoft Bulletins	Yes

Synopsis: Opening a specially crafted Microsoft Office file could result in arbitrary code execution.

Description: The remote Windows host does not include ClickOnce application file types in the Windows Packager unsafe file type list.

An attacker could leverage this issue to execute arbitrary code in the context of the current user on the affected host if he can trick the user into opening a Microsoft Office file with a malicious ClickOnce application embedded in it.

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-005

Risk Factor: High

STIG Severity: II

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.7

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2584146 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-0013

BID: 51284

Crossref: OSVDB #78207, MSFT #MS12-005, IAVA #2012-A-0007

Vulnerability Publication Date: 2012/01/10

Patch Publication Date: 2012/01/10

Plugin Publication Date: 2012/01/10

Plugin Modification Date: 2012/08/16

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-005.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks: Canvas (CANVAS), Metasploit (MS12-005 Microsoft Office ClickOnce Unsafe Object Package Handling Vulnerability)

Plugin	Plugin Name	Severity	Family	Exploit?
57474	MS12-006: Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584)	Medium	Windows : Microsoft Bulletins	Yes

Synopsis: It may be possibe to obtain sensitive information from the remote Windows host using the Secure Channel security package.

Description: A vulnerability exits in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted web traffic served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.

Solution: Microsoft has released a set of patches for XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-006

Risk Factor: Medium

STIG Severity: I

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2585542 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2011-3389

BID: 49778

Crossref: OSVDB #74829, MSFT #MS12-006, IAVB #2012-B-0006

Vulnerability Publication Date: 2011/09/06

Patch Publication Date: 2012/01/10

Plugin Publication Date: 2012/01/10

Plugin Modification Date: 2012/08/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-006.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
57942	MS12-008: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows kernel is affected by multiple remote code execution vulnerabilities.

Description: The remote host is running a version of the Windows kernel that is affected by multiple remote code execution vulnerabilities :

- Due to improper validation in input passed from user mode through the kernel component of GDI, an attacker can cause a denial of service condition or may be able to execute arbitrary code in kernel mode. (CVE-2011-5046)

- A flaw in the way the Windows kernel-mode drivers manages specific keyboard layouts could allow an attacker to run arbitrary code in kernel mode. (CVE-2012-0154)

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/Bulletin/MS12-008

See Also: http://www.exploit-db.com/exploits/18275

Risk Factor: High

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.4

CVSS Temporal Vector: CVSS2#E:POC/RL:U/RC:C

Plugin Output:
The host is missing KB 2660465 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2011-5046, CVE-2012-0154

BID: 51122, 51920

Crossref: OSVDB #77908, MSFT #MS12-008

Vulnerability Publication Date: 2011/12/18

Patch Publication Date: 2012/02/14

Plugin Publication Date: 2012/02/14

Plugin Modification Date: 2012/06/14

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-008.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
57943	MS12-009: Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host contains a driver that allows privilege escalation.

Description: The remote Windows host contains a version of the Ancillary Function Driver (afd.sys), which has multiple flaws that prevent it from properly validating input before passing it from user mode to the kernel.

An attacker with local access to the affected system could exploit these issues to execute arbitrary code in kernel mode and take complete control of the affected system.

Solution: Microsoft has released a set of patches for Windows XP x64, 2003, Vista, 2008 SP2, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-009

Risk Factor: High

STIG Severity: II

CVSS Base Score: 7.2

CVSS Vector: CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 6.0

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2645640 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-0148, CVE-2012-0149

BID: 51930, 51936

Crossref: OSVDB #79252, OSVDB #79253, MSFT #MS12-009, IAVB #2012-B-0021

Vulnerability Publication Date: 2012/02/14

Patch Publication Date: 2012/02/14

Plugin Publication Date: 2012/02/14

Plugin Modification Date: 2012/06/14

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-009.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
58331	MS12-019: Vulnerability in DirectWrite Could Allow Denial of Service (2665364)	Medium	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host is affected by a denial of service vulnerability.

Description: A denial of service vulnerability exists in the implementation of DirectWrite installed on the remote Windows host.

In an Instant Messenger-based attack scenario, an attacker sending a specially crafted sequence of Unicode characters directly to an Instant Messenger client could cause the application to become unresponsive.

Solution: Microsoft has released a set of patches for Windows Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-019

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSS Temporal Score: 4.1

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2665364 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-0156

BID: 52332

Crossref: OSVDB #80003, MSFT #MS12-019

Vulnerability Publication Date: 2012/03/13

Patch Publication Date: 2012/03/13

Plugin Publication Date: 2012/03/13

Plugin Modification Date: 2012/03/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-019.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
58332	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host could allow arbitrary code execution.

Description: An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted.

If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.

Note that the Remote Desktop Protocol is not enabled by default.

This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-020

See Also: http://aluigi.org/adv/termdd_1-adv.txt
http://www.zerodayinitiative.com/advisories/ZDI-12-044/

Risk Factor: High

STIG Severity: I

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.3

CVSS Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

Plugin Output:
The host is missing KB 2667402 according to WSUS.

CPE: cpe:/o:microsoft:windows
cpe:/a:microsoft:remote_desktop_protocol

CVE: CVE-2012-0002, CVE-2012-0152

BID: 52353, 52354

Crossref: OSVDB #80000, OSVDB #80004, CERT #624051, EDB-ID #18606, IAVA #2012-A-0039, MSFT #MS12-020

Vulnerability Publication Date: 2012/03/13

Patch Publication Date: 2012/03/13

Plugin Publication Date: 2012/03/13

Plugin Modification Date: 2012/08/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-020.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks: Canvas (White_Phosphorus), Metasploit (MS12-020 Microsoft Remote Desktop Use-After-Free DoS)

Plugin	Plugin Name	Severity	Family	Exploit?
58655	MS12-023: Cumulative Security Update for Internet Explorer (2675157)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote host is affected by code execution vulnerabilities.

Description: The remote host is missing Internet Explorer (IE) Security Update 2675157.

The installed version of IE is affected by several vulnerabilities that could allow an attacker to execute arbitrary code on the remote host.

Solution: Microsoft has released a set of patches for XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-023

See Also: http://www.zerodayinitiative.com/advisories/ZDI-12-065/
http://www.securityfocus.com/archive/1/522394/30/0/threaded

Risk Factor: High

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.8

CVSS Temporal Vector: CVSS2#E:F/RL:U/RC:ND

Plugin Output:
The host is missing KB 2675157 according to WSUS.

CPE: cpe:/a:microsoft:internet_explorer
cpe:/o:microsoft:windows

CVE: CVE-2012-0168, CVE-2012-0169, CVE-2012-0170, CVE-2012-0171, CVE-2012-0172

BID: 52889, 52890, 52904, 52905, 52906

Crossref: OSVDB #81126, OSVDB #81127, OSVDB #81128, OSVDB #81129, OSVDB #81130, MSFT #MS12-023

Vulnerability Publication Date: 2012/04/10

Patch Publication Date: 2012/04/10

Plugin Publication Date: 2012/04/11

Plugin Modification Date: 2012/07/12

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-023.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
59042	MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host is affected by multiple vulnerabilities.

Description: The remote Windows host is potentially affected by the following vulnerabilities :

- Multiple code execution vulnerabilities exist in the handling of specially crafted TrueType font files. (CVE-2011-3402, CVE-2012-0159)

- A code execution vulnerability exists in Microsoft .NET Framework that can allow a specially crafted Microsoft .NET Framework application to access memory in an unsafe manner. (CVE-2012-0162)

- A denial of service vulnerability exists in the way that .NET Framework compares the value of an index. (CVE-2012-0164)

- A code execution vulnerability exists in the way that GDI+ handles validation of specially crafted EMF images.
(CVE-2012-0165)

- A code execution vulnerability exists in the way that the Office GDI+ library handles validation of specially crafted EMF images embedded within an Office document.
(CVE-2012-0167)

- A code execution vulnerability exists in Microsoft Silverlight that can allow a specially crafted Silverlight application to access memory in an unsafe manner. (CVE-2012-0176)

- A privilege escalation vulnerability exists in the way that the Windows kernel-mode driver manages the functions related to Windows and Messages handling.
(CVE-2012-0180)

- A privilege escalation vulnerability exists in the way that the Windows kernel-mode driver manages Keyboard Layout files. (CVE-2012-0181)

- An unspecified privilege escalation vulnerability exists in the Windows kernel-mode driver. (CVE-2012-1848)

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, 2008 R2, Office 2003, 2007, and 2010, .NET Framework 3.0, 3.5.1, and 4.0, Silverlight 4, and 5 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-034

See Also: http://www.zerodayinitiative.com/advisories/ZDI-12-131
http://archives.neohapsis.com/archives/fulldisclosure/2012-08/0060.html

Risk Factor: High

STIG Severity: I

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.7

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2676562 according to WSUS.

CPE: cpe:/o:microsoft:windows
cpe:/a:microsoft:office

cpe:/a:microsoft:silverlight
cpe:/a:microsoft:.net_framework

CVE: CVE-2011-3402, CVE-2012-0159, CVE-2012-0162, CVE-2012-0164, CVE-2012-0165, CVE-2012-0167, CVE-2012-0176, CVE-2012-0180, CVE-2012-0181, CVE-2012-1848

BID: 50462, 53324, 53326, 53327, 53335, 53347, 53351, 53358, 53360, 53363

Crossref: OSVDB #76843, OSVDB #81715, OSVDB #81716, OSVDB #81717, OSVDB #81718, OSVDB #81719, OSVDB #81720, OSVDB #81721, OSVDB #81722, OSVDB #81736, MSFT #MS12-034, IAVA #2012-A-0079

Vulnerability Publication Date: 2012/05/08

Patch Publication Date: 2012/05/08

Plugin Publication Date: 2012/05/09

Plugin Modification Date: 2012/08/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-034.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks: Metasploit (Windows Gather Forensics Duqu Registry Check)

Plugin	Plugin Name	Severity	Family	Exploit?
59455	MS12-037: Cumulative Security Update for Internet Explorer (2699988)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote host is affected by code execution vulnerabilities.

Description: The remote host is missing Internet Explorer (IE) Security Update 2699988.

The installed version of IE is affected by several vulnerabilities that could allow an attacker to execute arbitrary code on the remote host.

Solution: Microsoft has released a set of patches for XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-037

See Also: http://www.nessus.org/u?c7d49512
http://www.nessus.org/u?18c6adba
http://www.zerodayinitiative.com/advisories/ZDI-12-093/
http://www.securityfocus.com/archive/1/523185/30/0/threaded
http://www.securityfocus.com/archive/1/523186/30/0/threaded
http://www.securityfocus.com/archive/1/523196/30/0/threaded

Risk Factor: High

STIG Severity: II

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

Plugin Output:
The host is missing KB 2699988 according to WSUS.

CPE: cpe:/a:microsoft:internet_explorer
cpe:/o:microsoft:windows

CVE: CVE-2012-1523, CVE-2012-1858, CVE-2012-1872, CVE-2012-1873, CVE-2012-1874, CVE-2012-1875, CVE-2012-1876, CVE-2012-1877, CVE-2012-1878, CVE-2012-1879, CVE-2012-1880, CVE-2012-1881, CVE-2012-1882

BID: 53841, 53842, 53843, 53844, 53845, 53847, 53848, 53866, 53867, 53868, 53869, 53870, 53871

Crossref: OSVDB #82860, OSVDB #82861, OSVDB #82862, OSVDB #82863, OSVDB #82864, OSVDB #82865, OSVDB #82866, OSVDB #82867, OSVDB #82868, OSVDB #82869, OSVDB #82870, OSVDB #82871, OSVDB #82872, EDB-ID #19777, IAVB #2012-B-0066, EDB-ID #20174, MSFT #MS12-037

Vulnerability Publication Date: 2012/06/12

Patch Publication Date: 2012/06/12

Plugin Publication Date: 2012/06/13

Plugin Modification Date: 2012/08/18

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-037.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks: Metasploit (Microsoft Internet Explorer Fixed Table Col Span Heap Overflow)

Plugin	Plugin Name	Severity	Family	Exploit?
59456	MS12-038: Vulnerability in .NET Framework Could Allow Remote Code Execution (2706726)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The .NET Framework installed on the remote Windows host could allow arbitrary code execution.

Description: The version of the .NET Framework installed on the remote host is affected by a code execution vulnerability due to the improper execution of a function pointer.

A remote, unauthenticated attacker could execute arbitrary code on the remote host subject to the privileges of the user running the affected application.

Solution: Microsoft has released a set of patches for .NET Framework 2.0, 3.5, and 4 :

http://technet.microsoft.com/en-us/security/Bulletin/MS12-038

See Also: http://www.zerodayinitiative.com/advisories/ZDI-12-141/
http://www.securityfocus.com/archive/1/523936/30/0/threaded

Risk Factor: High

STIG Severity: II

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 6.9

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:
The host is missing KB 2686831 according to WSUS.

CPE: cpe:/o:microsoft:windows
cpe:/a:microsoft:.net_framework

CVE: CVE-2012-1855

BID: 53861

Crossref: OSVDB #82859, MSFT #MS12-038, IAVA #2012-A-0091

Vulnerability Publication Date: 2012/06/12

Patch Publication Date: 2012/06/12

Plugin Publication Date: 2012/06/13

Plugin Modification Date: 2012/08/20

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: local

Source File: smb_nt_ms12-038.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
59460	MS12-042: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2711167)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The Windows kernel is affected by a multiple vulnerabilities that could result in privilege escalation.

Description: The remote host is running a Windows kernel version that is affected by multiple privilege escalation vulnerabilities:

- A vulnerability exists in the way that the Windows User Mode Scheduler handles system requests that can be exploited to execute arbitrary code in kernel mode. (CVE-2012-0217)

- A vulnerability exists in the way that Windows handles BIOS memory that can be exploited to execute arbitrary code in kernel mode. (CVE-2012-1515)

Solution: Microsoft has released a set of patches for 32-bit versions of Windows XP and 2003 as well as patches for 64-bit versions of Windows 7 and Server 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/MS12-042

Risk Factor: High

STIG Severity: I

CVSS Base Score: 7.2

CVSS Vector: CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 5.3

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:
The host is missing KB 2709715 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-0217, CVE-2012-1515

BID: 52820, 53856

Crossref: OSVDB #82849, OSVDB #82850, MSFT #MS12-042, IAVA #2012-A-0055

Vulnerability Publication Date: 2012/03/19

Patch Publication Date: 2012/06/12

Plugin Publication Date: 2012/06/13

Plugin Modification Date: 2012/06/17

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: local

Source File: smb_nt_ms12-042.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
59906	MS12-043: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)	High	Windows : Microsoft Bulletins	Yes

Synopsis: Arbitrary code can be executed on the remote host through Microsoft XML Core Services.

Description: The version of Microsoft XML Core Services installed on the remote Windows host is affected by a remote code execution vulnerability that could allow arbitrary code execution if a user views a specially crafted web page using Internet Explorer.

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-043

Risk Factor: High

STIG Severity: I

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.4

CVSS Temporal Vector: CVSS2#E:F/RL:W/RC:C

Plugin Output:
The host is missing KB 2719985 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-1889

BID: 53934

Crossref: OSVDB #82873, MSFT #MS12-043, IAVA #2012-A-0111

Vulnerability Publication Date: 2012/07/10

Patch Publication Date: 2012/07/10

Plugin Publication Date: 2012/07/11

Plugin Modification Date: 2012/08/16

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-043.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks: Metasploit (MS12-043 Microsoft XML Core Services MSXML Uninitialized Memory Corruption)

Plugin	Plugin Name	Severity	Family	Exploit?
59912	MS12-049: Vulnerability in TLS Could Allow Information Disclosure (2655992)	Medium	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host has an information disclosure vulnerability.

Description: A design flaw in the CBC mode of operation on the TLS protocol can allow encrypted TLS traffic to be decrypted. This vulnerability could allow for the decryption of HTTPS traffic by an unauthorized third party.

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/MS12-049

Risk Factor: Medium

STIG Severity: II

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2655992 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-1870

BID: 54304

Crossref: OSVDB #83660, MSFT #MS12-049, IAVA #2012-A-0108

Vulnerability Publication Date: 2012/07/10

Patch Publication Date: 2012/07/10

Plugin Publication Date: 2012/07/11

Plugin Modification Date: 2012/07/14

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-049.nasl

First Discovered: Aug 26, 2012 17:27:39 CDT

Last Observed: Aug 26, 2012 17:27:39 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
61529	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host is potentially affected by multiple code execution vulnerabilities.

Description: The remote Windows host is potentially affected by the following vulnerabilities :

- A denial of service vulnerability exists in Windows networking components. The vulnerability is due to the service not properly handling specially crafted RAP requests. (CVE-2012-1850)

- A remote code execution vulnerability exists in the Windows Print Spooler service that can allow a remote, unauthenticated attacker to execute arbitrary code on an affected system. (CVE-2012-1851)

- A remote code execution vulnerability exists in the way that Windows networking components handle specially crafted RAP responses.
(CVE-2012-1852, CVE-2012-1853)

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-054

Risk Factor: Critical

STIG Severity: I

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.3

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2712808 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-1850, CVE-2012-1851, CVE-2012-1852, CVE-2012-1853

BID: 54921, 54928, 54931, 54940

Crossref: OSVDB #84598, OSVDB #84599, OSVDB #84600, OSVDB #84601, MSFT #MS12-054, IAVA #2012-A-0137

Vulnerability Publication Date: 2012/08/14

Patch Publication Date: 2012/08/14

Plugin Publication Date: 2012/08/15

Plugin Modification Date: 2012/08/18

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-054.nasl
First Discovered: Aug 26, 2012 17:27:39 CDT
Last Observed: Aug 26, 2012 17:27:39 CDT
Exploit Frameworks:

10.0.0.116

NetBIOS Name: ITSDEPT\DT0004-PC
MAC Address: 08:00:27:68:c4:5b
DNS Name: dt0004-pc.itsdept.com
Repository: wsus
Last Scan: Aug 30, 2012 @ 1:37AM

Details

Plugin	Plugin Name	Severity	Family	Exploit?
57942	MS12-008: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows kernel is affected by multiple remote code execution vulnerabilities.

Description: The remote host is running a version of the Windows kernel that is affected by multiple remote code execution vulnerabilities :

- Due to improper validation in input passed from user mode through the kernel component of GDI, an attacker can cause a denial of service condition or may be able to execute arbitrary code in kernel mode. (CVE-2011-5046)

- A flaw in the way the Windows kernel-mode drivers manages specific keyboard layouts could allow an attacker to run arbitrary code in kernel mode. (CVE-2012-0154)

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/Bulletin/MS12-008

See Also: http://www.exploit-db.com/exploits/18275

Risk Factor: High

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.4

CVSS Temporal Vector: CVSS2#E:POC/RL:U/RC:C

Plugin Output:
The host is missing KB 2660465 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2011-5046, CVE-2012-0154

BID: 51122, 51920

Crossref: OSVDB #77908, MSFT #MS12-008

Vulnerability Publication Date: 2011/12/18

Patch Publication Date: 2012/02/14

Plugin Publication Date: 2012/02/14

Plugin Modification Date: 2012/06/14

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-008.nasl

First Discovered: Aug 22, 2012 22:10:19 CDT

Last Observed: Aug 22, 2012 22:10:19 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
57943	MS12-009: Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host contains a driver that allows privilege escalation.

Description: The remote Windows host contains a version of the Ancillary Function Driver (afd.sys), which has multiple flaws that prevent it from properly validating input before passing it from user mode to the kernel.

An attacker with local access to the affected system could exploit these issues to execute arbitrary code in kernel mode and take complete control of the affected system.

Solution: Microsoft has released a set of patches for Windows XP x64, 2003, Vista, 2008 SP2, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-009

Risk Factor: High

STIG Severity: II

CVSS Base Score: 7.2

CVSS Vector: CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 6.0

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2645640 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-0148, CVE-2012-0149

BID: 51930, 51936

Crossref: OSVDB #79252, OSVDB #79253, MSFT #MS12-009, IAVB #2012-B-0021

Vulnerability Publication Date: 2012/02/14

Patch Publication Date: 2012/02/14

Plugin Publication Date: 2012/02/14

Plugin Modification Date: 2012/06/14

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-009.nasl

First Discovered: Aug 22, 2012 22:10:19 CDT

Last Observed: Aug 22, 2012 22:10:19 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
58331	MS12-019: Vulnerability in DirectWrite Could Allow Denial of Service (2665364)	Medium	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host is affected by a denial of service vulnerability.

Description: A denial of service vulnerability exists in the implementation of DirectWrite installed on the remote Windows host.

In an Instant Messenger-based attack scenario, an attacker sending a specially crafted sequence of Unicode characters directly to an Instant Messenger client could cause the application to become unresponsive.

Solution: Microsoft has released a set of patches for Windows Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-019

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSS Temporal Score: 4.1

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2665364 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-0156

BID: 52332

Crossref: OSVDB #80003, MSFT #MS12-019

Vulnerability Publication Date: 2012/03/13

Patch Publication Date: 2012/03/13

Plugin Publication Date: 2012/03/13

Plugin Modification Date: 2012/03/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-019.nasl

First Discovered: Aug 22, 2012 22:10:19 CDT

Last Observed: Aug 22, 2012 22:10:19 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
58332	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host could allow arbitrary code execution.

Description: An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted.

If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.

Note that the Remote Desktop Protocol is not enabled by default.

This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-020

See Also: http://aluigi.org/adv/termdd_1-adv.txt

http://www.zerodayinitiative.com/advisories/ZDI-12-044/

Risk Factor: High

STIG Severity: I

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.3

CVSS Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

Plugin Output:
The host is missing KB 2667402 according to WSUS.

CPE: cpe:/o:microsoft:windows
cpe:/a:microsoft:remote_desktop_protocol

CVE: CVE-2012-0002, CVE-2012-0152

BID: 52353, 52354

Crossref: OSVDB #80000, OSVDB #80004, CERT #624051, EDB-ID #18606, IAVA #2012-A-0039, MSFT #MS12-020

Vulnerability Publication Date: 2012/03/13

Patch Publication Date: 2012/03/13

Plugin Publication Date: 2012/03/13

Plugin Modification Date: 2012/08/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-020.nasl

First Discovered: Aug 22, 2012 22:10:19 CDT

Last Observed: Aug 22, 2012 22:10:19 CDT

Exploit Frameworks: Canvas (White_Phosphorus), Metasploit (MS12-020 Microsoft Remote Desktop Use-After-Free DoS)

Plugin	Plugin Name	Severity	Family	Exploit?
58655	MS12-023: Cumulative Security Update for Internet Explorer (2675157)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote host is affected by code execution vulnerabilities.

Description: The remote host is missing Internet Explorer (IE) Security Update 2675157.

The installed version of IE is affected by several vulnerabilities that could allow an attacker to execute arbitrary code on the remote host.

Solution: Microsoft has released a set of patches for XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-023

See Also: http://www.zerodayinitiative.com/advisories/ZDI-12-065/
http://www.securityfocus.com/archive/1/522394/30/0/threaded

Risk Factor: High

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.8

CVSS Temporal Vector: CVSS2#E:F/RL:U/RC:ND

Plugin Output:
The host is missing KB 2675157 according to WSUS.

CPE: cpe:/a:microsoft:internet_explorer
cpe:/o:microsoft:windows

CVE: CVE-2012-0168, CVE-2012-0169, CVE-2012-0170, CVE-2012-0171, CVE-2012-0172

BID: 52889, 52890, 52904, 52905, 52906

Crossref: OSVDB #81126, OSVDB #81127, OSVDB #81128, OSVDB #81129, OSVDB #81130, MSFT #MS12-023

Vulnerability Publication Date: 2012/04/10

Patch Publication Date: 2012/04/10

Plugin Publication Date: 2012/04/11

Plugin Modification Date: 2012/07/12

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-023.nasl

First Discovered: Aug 22, 2012 22:10:19 CDT

Last Observed: Aug 22, 2012 22:10:19 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
59042	MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host is affected by multiple vulnerabilities.

Description: The remote Windows host is potentially affected by the following vulnerabilities :

- Multiple code execution vulnerabilities exist in the handling of specially crafted TrueType font files. (CVE-2011-3402, CVE-2012-0159)

- A code execution vulnerability exists in Microsoft .NET Framework that can allow a specially crafted Microsoft .NET Framework application to access memory in an unsafe manner. (CVE-2012-0162)

- A denial of service vulnerability exists in the way that .NET Framework compares the value of an index. (CVE-2012-0164)

- A code execution vulnerability exists in the way that GDI+ handles validation of specially crafted EMF images. (CVE-2012-0165)

- A code execution vulnerability exists in the way that the Office GDI+ library handles validation of specially crafted EMF images embedded within an Office document. (CVE-2012-0167)

- A code execution vulnerability exists in Microsoft Silverlight that can allow a specially crafted Silverlight application to access memory in an unsafe manner. (CVE-2012-0176)

- A privilege escalation vulnerability exists in the way that the Windows kernel-mode driver manages the functions related to Windows and Messages handling. (CVE-2012-0180)

- A privilege escalation vulnerability exists in the way that the Windows kernel-mode driver manages Keyboard Layout files. (CVE-2012-0181)

- An unspecified privilege escalation vulnerability exists in the Windows kernel-mode driver. (CVE-2012-1848)

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, 2008 R2, Office 2003, 2007, and 2010, .NET Framework 3.0, 3.5.1, and 4.0, Silverlight 4, and 5 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-034

See Also: http://www.zerodayinitiative.com/advisories/ZDI-12-131
http://archives.neohapsis.com/archives/fulldisclosure/2012-08/0060.html

Risk Factor: High

STIG Severity: I

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.7

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2676562 according to WSUS.

CPE: cpe:/o:microsoft:windows
cpe:/a:microsoft:office
cpe:/a:microsoft:silverlight
cpe:/a:microsoft:.net_framework

CVE: CVE-2011-3402, CVE-2012-0159, CVE-2012-0162, CVE-2012-0164, CVE-2012-0165, CVE-2012-0167, CVE-2012-0176, CVE-2012-0180, CVE-2012-0181, CVE-2012-1848

BID: 50462, 53324, 53326, 53327, 53335, 53347, 53351, 53358, 53360, 53363

Crossref: OSVDB #76843, OSVDB #81715, OSVDB #81716, OSVDB #81717, OSVDB #81718, OSVDB #81719, OSVDB #81720, OSVDB #81721, OSVDB #81722, OSVDB #81736, MSFT #MS12-034, IAVA #2012-A-0079

Vulnerability Publication Date: 2012/05/08

Patch Publication Date: 2012/05/08

Plugin Publication Date: 2012/05/09

Plugin Modification Date: 2012/08/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-034.nasl

First Discovered: Aug 22, 2012 22:10:19 CDT

Last Observed: Aug 22, 2012 22:10:19 CDT

Exploit Frameworks: Metasploit (Windows Gather Forensics Duqu Registry Check)

Plugin	Plugin Name	Severity	Family	Exploit?
59455	MS12-037: Cumulative Security Update for Internet Explorer (2699988)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote host is affected by code execution vulnerabilities.

Description: The remote host is missing Internet Explorer (IE) Security Update 2699988.

The installed version of IE is affected by several vulnerabilities that could allow an attacker to execute arbitrary code on the remote host.

Solution: Microsoft has released a set of patches for XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-037

See Also: http://www.nessus.org/u?c7d49512
http://www.nessus.org/u?18c6adba
http://www.zerodayinitiative.com/advisories/ZDI-12-093/
http://www.securityfocus.com/archive/1/523185/30/0/threaded
http://www.securityfocus.com/archive/1/523186/30/0/threaded
http://www.securityfocus.com/archive/1/523196/30/0/threaded

Risk Factor: High

STIG Severity: II

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

Plugin Output:
The host is missing KB 2699988 according to WSUS.

CPE: cpe:/a:microsoft:internet_explorer
cpe:/o:microsoft:windows

CVE: CVE-2012-1523, CVE-2012-1858, CVE-2012-1872, CVE-2012-1873, CVE-2012-1874, CVE-2012-1875, CVE-2012-1876, CVE-2012-1877, CVE-2012-1878, CVE-2012-1879, CVE-2012-1880, CVE-2012-1881, CVE-2012-1882

BID: 53841, 53842, 53843, 53844, 53845, 53847, 53848, 53866, 53867, 53868, 53869, 53870, 53871

Crossref: OSVDB #82860, OSVDB #82861, OSVDB #82862, OSVDB #82863, OSVDB #82864, OSVDB #82865, OSVDB #82866, OSVDB #82867, OSVDB #82868, OSVDB #82869, OSVDB #82870, OSVDB #82871, OSVDB #82872, EDB-ID #19777, IAVB #2012-B-0066, EDB-ID #20174, MSFT #MS12-037

Vulnerability Publication Date: 2012/06/12

Patch Publication Date: 2012/06/12

Plugin Publication Date: 2012/06/13

Plugin Modification Date: 2012/08/18

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-037.nasl

First Discovered: Aug 22, 2012 22:10:19 CDT

Last Observed: Aug 22, 2012 22:10:19 CDT

Exploit Frameworks: Metasploit (Microsoft Internet Explorer Fixed Table Col Span Heap Overflow)

Plugin	Plugin Name	Severity	Family	Exploit?
59456	MS12-038: Vulnerability in .NET Framework Could Allow Remote Code Execution (2706726)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The .NET Framework installed on the remote Windows host could allow arbitrary code execution.

Description: The version of the .NET Framework installed on the remote host is affected by a code execution vulnerability due to the improper execution of a function pointer.

A remote, unauthenticated attacker could execute arbitrary code on the remote host subject to the privileges of the user running the affected application.

Solution: Microsoft has released a set of patches for .NET Framework 2.0, 3.5, and 4 :

http://technet.microsoft.com/en-us/security/Bulletin/MS12-038

See Also: http://www.zerodayinitiative.com/advisories/ZDI-12-141/
http://www.securityfocus.com/archive/1/523936/30/0/threaded

Risk Factor: High

STIG Severity: II

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 6.9

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:
The host is missing KB 2686831 according to WSUS.

CPE: cpe:/o:microsoft:windows
cpe:/a:microsoft:.net_framework

CVE: CVE-2012-1855

BID: 53861

Crossref: OSVDB #82859, MSFT #MS12-038, IAVA #2012-A-0091

Vulnerability Publication Date: 2012/06/12

Patch Publication Date: 2012/06/12

Plugin Publication Date: 2012/06/13

Plugin Modification Date: 2012/08/20

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: local

Source File: smb_nt_ms12-038.nasl

First Discovered: Aug 22, 2012 22:10:19 CDT

Last Observed: Aug 22, 2012 22:10:19 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
59460	MS12-042: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2711167)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The Windows kernel is affected by a multiple vulnerabilities that could result in privilege escalation.

Description: The remote host is running a Windows kernel version that is affected by multiple privilege escalation vulnerabilities:

- A vulnerability exists in the way that the Windows User Mode Scheduler handles system requests that can be exploited to execute arbitrary code in kernel mode. (CVE-2012-0217)

- A vulnerability exists in the way that Windows handles BIOS memory that can be exploited to execute arbitrary code in kernel mode. (CVE-2012-1515)

Solution: Microsoft has released a set of patches for 32-bit versions of Windows XP and 2003 as well as patches for 64-bit versions of Windows 7 and Server 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/MS12-042

Risk Factor: High

STIG Severity: I

CVSS Base Score: 7.2

CVSS Vector: CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 5.3

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:
The host is missing KB 2709715 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-0217, CVE-2012-1515

BID: 52820, 53856

Crossref: OSVDB #82849, OSVDB #82850, MSFT #MS12-042, IAVA #2012-A-0055

Vulnerability Publication Date: 2012/03/19

Patch Publication Date: 2012/06/12

Plugin Publication Date: 2012/06/13

Plugin Modification Date: 2012/06/17

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: local

Source File: smb_nt_ms12-042.nasl

First Discovered: Aug 22, 2012 22:10:19 CDT

Last Observed: Aug 22, 2012 22:10:19 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
59906	MS12-043: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)	High	Windows : Microsoft Bulletins	Yes

Synopsis: Arbitrary code can be executed on the remote host through Microsoft XML Core Services.

Description: The version of Microsoft XML Core Services installed on the remote Windows host is affected by a remote code execution vulnerability that could allow arbitrary code execution if a user views a specially crafted web page using Internet Explorer.

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-043

Risk Factor: High

STIG Severity: I

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.4

CVSS Temporal Vector: CVSS2#E:F/RL:W/RC:C

Plugin Output:
The host is missing KB 2719985 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-1889

BID: 53934

Crossref: OSVDB #82873, MSFT #MS12-043, IAVA #2012-A-0111

Vulnerability Publication Date: 2012/07/10

Patch Publication Date: 2012/07/10

Plugin Publication Date: 2012/07/11

Plugin Modification Date: 2012/08/16

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-043.nasl

First Discovered: Aug 22, 2012 22:10:19 CDT

Last Observed: Aug 22, 2012 22:10:19 CDT

Exploit Frameworks: Metasploit (MS12-043 Microsoft XML Core Services MSXML Uninitialized Memory Corruption)

Plugin	Plugin Name	Severity	Family	Exploit?
59912	MS12-049: Vulnerability in TLS Could Allow Information Disclosure (2655992)	Medium	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host has an information disclosure vulnerability.

Description: A design flaw in the CBC mode of operation on the TLS protocol can allow encrypted TLS traffic to be decrypted. This vulnerability could allow for the decryption of HTTPS traffic by an unauthorized third party.

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/MS12-049

Risk Factor: Medium

STIG Severity: II

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2655992 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-1870

BID: 54304

Crossref: OSVDB #83660, MSFT #MS12-049, IAVA #2012-A-0108

Vulnerability Publication Date: 2012/07/10

Patch Publication Date: 2012/07/10

Plugin Publication Date: 2012/07/11

Plugin Modification Date: 2012/07/14

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-049.nasl

First Discovered: Aug 22, 2012 22:10:19 CDT

Last Observed: Aug 22, 2012 22:10:19 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
61529	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host is potentially affected by multiple code execution vulnerabilities.

Description: The remote Windows host is potentially affected by the following vulnerabilities :

- A denial of service vulnerability exists in Windows networking components. The vulnerability is due to the service not properly handling specially crafted RAP requests. (CVE-2012-1850)

- A remote code execution vulnerability exists in the Windows Print Spooler service that can allow a remote, unauthenticated attacker to execute arbitrary code on an affected system. (CVE-2012-1851)

- A remote code execution vulnerability exists in the way that Windows networking components handle specially crafted RAP responses. (CVE-2012-1852, CVE-2012-1853)

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-054

Risk Factor: Critical

STIG Severity: I

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.3

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2712808 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-1850, CVE-2012-1851, CVE-2012-1852, CVE-2012-1853

BID: 54921, 54928, 54931, 54940

Crossref: OSVDB #84598, OSVDB #84599, OSVDB #84600, OSVDB #84601, MSFT #MS12-054, IAVA #2012-A-0137

Vulnerability Publication Date: 2012/08/14

Patch Publication Date: 2012/08/14

Plugin Publication Date: 2012/08/15

Plugin Modification Date: 2012/08/18

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-054.nasl

First Discovered: Aug 22, 2012 22:10:19 CDT

Last Observed: Aug 22, 2012 22:10:19 CDT

Exploit Frameworks:

10.0.0.113

NetBIOS Name: ITSDEPT\DT0001-PC
MAC Address: 08:00:27:29:cd:93
DNS Name: dt0001-pc.itsdept.com
Repository: wsus
Last Scan: Aug 30, 2012 @ 1:37AM

Details

Plugin	Plugin Name	Severity	Family	Exploit?
57472	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391)	High	Windows : Microsoft Bulletins	Yes

Synopsis: Opening a specially crafted media file could result in arbitrary code execution.

Description: The version of Windows Media installed on the remote host is affected by one or both of the following vulnerabilities :

- The Winmm.dll library as used by Windows Media Player does not properly handle specially crafted MIDI files. (CVE-2012-0003)

- A DirectShow component of DirectX does not properly handle specially crafted media files. (CVE-2012-0004)

An attacker who tricked a user on the affected host into opening a specially crafted MIDI or media file could leverage these issues to execute arbitrary code in the context of the current user.

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 as well as Windows XP Media Center Edition 2005 and Windows Media Center TV Pack 2008 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-004

Risk Factor: High

STIG Severity: II

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.7

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2631813 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-0003, CVE-2012-0004

BID: 51292, 51295

Crossref: OSVDB #78210, OSVDB #78211, EDB-ID #18426, MSFT #MS12-004, IAVA #2012-A-0005

Vulnerability Publication Date: 2012/01/10

Patch Publication Date: 2012/01/10

Plugin Publication Date: 2012/01/10

Plugin Modification Date: 2012/08/16

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-004.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks: Metasploit (MS12-004 midiOutPlayNextPolyEvent Heap Overflow)

Plugin	Plugin Name	Severity	Family	Exploit?
57473	MS12-005: Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146)	High	Windows : Microsoft Bulletins	Yes

Synopsis: Opening a specially crafted Microsoft Office file could result in arbitrary code execution.

Description: The remote Windows host does not include ClickOnce application file types in the Windows Packager unsafe file type list.

An attacker could leverage this issue to execute arbitrary code in the context of the current user on the affected host if he can trick the user into opening a Microsoft Office file with a malicious ClickOnce application embedded in it.

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-005

Risk Factor: High

STIG Severity: II

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.7

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2584146 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-0013

BID: 51284

Crossref: OSVDB #78207, MSFT #MS12-005, IAVA #2012-A-0007

Vulnerability Publication Date: 2012/01/10

Patch Publication Date: 2012/01/10

Plugin Publication Date: 2012/01/10

Plugin Modification Date: 2012/08/16

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-005.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks: Canvas (CANVAS), Metasploit (MS12-005 Microsoft Office ClickOnce Unsafe Object Package Handling Vulnerability)

Plugin	Plugin Name	Severity	Family	Exploit?
57474	MS12-006: Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584)	Medium	Windows : Microsoft Bulletins	Yes

Synopsis: It may be possibe to obtain sensitive information from the remote Windows host using the Secure Channel security package.

Description: A vulnerability exits in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted web traffic served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.

Solution: Microsoft has released a set of patches for XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-006

Risk Factor: Medium

STIG Severity: I

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2585542 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2011-3389

BID: 49778

Crossref: OSVDB #74829, MSFT #MS12-006, IAVB #2012-B-0006

Vulnerability Publication Date: 2011/09/06

Patch Publication Date: 2012/01/10

Plugin Publication Date: 2012/01/10

Plugin Modification Date: 2012/08/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-006.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
57942	MS12-008: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows kernel is affected by multiple remote code execution vulnerabilities.

Description: The remote host is running a version of the Windows kernel that is affected by multiple remote code execution vulnerabilities :

- Due to improper validation in input passed from user mode through the kernel component of GDI, an attacker can cause a denial of service condition or may be able to execute arbitrary code in kernel mode. (CVE-2011-5046)

- A flaw in the way the Windows kernel-mode drivers manages specific keyboard layouts could allow an attacker to run arbitrary code in kernel mode. (CVE-2012-0154)

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/Bulletin/MS12-008

See Also: http://www.exploit-db.com/exploits/18275

Risk Factor: High

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.4

CVSS Temporal Vector: CVSS2#E:POC/RL:U/RC:C

Plugin Output:
The host is missing KB 2660465 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2011-5046, CVE-2012-0154

BID: 51122, 51920

Crossref: OSVDB #77908, MSFT #MS12-008

Vulnerability Publication Date: 2011/12/18

Patch Publication Date: 2012/02/14

Plugin Publication Date: 2012/02/14

Plugin Modification Date: 2012/06/14

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-008.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
57943	MS12-009: Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host contains a driver that allows privilege escalation.

Description: The remote Windows host contains a version of the Ancillary Function Driver (afd.sys), which has multiple flaws that prevent it from properly validating input before passing it from user mode to the kernel.

An attacker with local access to the affected system could exploit these issues to execute arbitrary code in kernel mode and take complete control of the affected system.

Solution: Microsoft has released a set of patches for Windows XP x64, 2003, Vista, 2008 SP2, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-009

Risk Factor: High

STIG Severity: II

CVSS Base Score: 7.2

CVSS Vector: CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 6.0

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2645640 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-0148, CVE-2012-0149

BID: 51930, 51936

Crossref: OSVDB #79252, OSVDB #79253, MSFT #MS12-009, IAVB #2012-B-0021

Vulnerability Publication Date: 2012/02/14

Patch Publication Date: 2012/02/14

Plugin Publication Date: 2012/02/14

Plugin Modification Date: 2012/06/14

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-009.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
58331	MS12-019: Vulnerability in DirectWrite Could Allow Denial of Service (2665364)	Medium	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host is affected by a denial of service vulnerability.

Description: A denial of service vulnerability exists in the implementation of DirectWrite installed on the remote Windows host.

In an Instant Messenger-based attack scenario, an attacker sending a specially crafted sequence of Unicode characters directly to an Instant Messenger client could cause the application to become unresponsive.

Solution: Microsoft has released a set of patches for Windows Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-019

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSS Temporal Score: 4.1

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2665364 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-0156

BID: 52332

Crossref: OSVDB #80003, MSFT #MS12-019

Vulnerability Publication Date: 2012/03/13

Patch Publication Date: 2012/03/13

Plugin Publication Date: 2012/03/13

Plugin Modification Date: 2012/03/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-019.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
58332	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host could allow arbitrary code execution.

Description: An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted.

If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.

Note that the Remote Desktop Protocol is not enabled by default.

This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-020

See Also: http://aluigi.org/adv/termdd_1-adv.txt
http://www.zerodayinitiative.com/advisories/ZDI-12-044/

Risk Factor: High

STIG Severity: I

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.3

CVSS Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

Plugin Output:
The host is missing KB 2667402 according to WSUS.

CPE: cpe:/o:microsoft:windows
cpe:/a:microsoft:remote_desktop_protocol

CVE: CVE-2012-0002, CVE-2012-0152

BID: 52353, 52354

Crossref: OSVDB #80000, OSVDB #80004, CERT #624051, EDB-ID #18606, IAVA #2012-A-0039, MSFT #MS12-020

Vulnerability Publication Date: 2012/03/13

Patch Publication Date: 2012/03/13

Plugin Publication Date: 2012/03/13

Plugin Modification Date: 2012/08/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-020.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks: Canvas (White_Phosphorus), Metasploit (MS12-020 Microsoft Remote Desktop Use-After-Free DoS)

Plugin	Plugin Name	Severity	Family	Exploit?
58655	MS12-023: Cumulative Security Update for Internet Explorer (2675157)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote host is affected by code execution vulnerabilities.

Description: The remote host is missing Internet Explorer (IE) Security Update 2675157.

The installed version of IE is affected by several vulnerabilities that could allow an attacker to execute arbitrary code on the remote host.

Solution: Microsoft has released a set of patches for XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-023

See Also: http://www.zerodayinitiative.com/advisories/ZDI-12-065/
http://www.securityfocus.com/archive/1/522394/30/0/threaded

Risk Factor: High

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.8

CVSS Temporal Vector: CVSS2#E:F/RL:U/RC:ND

Plugin Output:
The host is missing KB 2675157 according to WSUS.

CPE: cpe:/a:microsoft:internet_explorer
cpe:/o:microsoft:windows

CVE: CVE-2012-0168, CVE-2012-0169, CVE-2012-0170, CVE-2012-0171, CVE-2012-0172

BID: 52889, 52890, 52904, 52905, 52906

Crossref: OSVDB #81126, OSVDB #81127, OSVDB #81128, OSVDB #81129, OSVDB #81130, MSFT #MS12-023

Vulnerability Publication Date: 2012/04/10

Patch Publication Date: 2012/04/10

Plugin Publication Date: 2012/04/11

Plugin Modification Date: 2012/07/12

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-023.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
59042	MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host is affected by multiple vulnerabilities.

Description: The remote Windows host is potentially affected by the following vulnerabilities :

- Multiple code execution vulnerabilities exist in the handling of specially crafted TrueType font files. (CVE-2011-3402, CVE-2012-0159)

- A code execution vulnerability exists in Microsoft .NET Framework that can allow a specially crafted Microsoft .NET Framework application to access memory in an unsafe manner. (CVE-2012-0162)

- A denial of service vulnerability exists in the way that .NET Framework compares the value of an index. (CVE-2012-0164)

- A code execution vulnerability exists in the way that GDI+ handles validation of specially crafted EMF images.
(CVE-2012-0165)

- A code execution vulnerability exists in the way that the Office GDI+ library handles validation of specially crafted EMF images embedded within an Office document.
(CVE-2012-0167)

- A code execution vulnerability exists in Microsoft Silverlight that can allow a specially crafted Silverlight application to access memory in an unsafe manner. (CVE-2012-0176)

- A privilege escalation vulnerability exists in the way that the Windows kernel-mode driver manages the functions related to Windows and Messages handling.
(CVE-2012-0180)

- A privilege escalation vulnerability exists in the way that the Windows kernel-mode driver manages Keyboard Layout files. (CVE-2012-0181)

- An unspecified privilege escalation vulnerability exists in the Windows kernel-mode driver. (CVE-2012-1848)

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, 2008 R2, Office 2003, 2007, and 2010, .NET Framework 3.0, 3.5.1, and 4.0, Silverlight 4, and 5 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-034

See Also: http://www.zerodayinitiative.com/advisories/ZDI-12-131
http://archives.neohapsis.com/archives/fulldisclosure/2012-08/0060.html

Risk Factor: High

STIG Severity: I

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.7

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2676562 according to WSUS.

CPE: cpe:/o:microsoft:windows
cpe:/a:microsoft:office

cpe:/a:microsoft:silverlight
cpe:/a:microsoft:.net_framework

CVE: CVE-2011-3402, CVE-2012-0159, CVE-2012-0162, CVE-2012-0164, CVE-2012-0165, CVE-2012-0167, CVE-2012-0176, CVE-2012-0180, CVE-2012-0181, CVE-2012-1848

BID: 50462, 53324, 53326, 53327, 53335, 53347, 53351, 53358, 53360, 53363

Crossref: OSVDB #76843, OSVDB #81715, OSVDB #81716, OSVDB #81717, OSVDB #81718, OSVDB #81719, OSVDB #81720, OSVDB #81721, OSVDB #81722, OSVDB #81736, MSFT #MS12-034, IAVA #2012-A-0079

Vulnerability Publication Date: 2012/05/08

Patch Publication Date: 2012/05/08

Plugin Publication Date: 2012/05/09

Plugin Modification Date: 2012/08/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-034.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks: Metasploit (Windows Gather Forensics Duqu Registry Check)

Plugin	Plugin Name	Severity	Family	Exploit?
59455	MS12-037: Cumulative Security Update for Internet Explorer (2699988)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The remote host is affected by code execution vulnerabilities.

Description: The remote host is missing Internet Explorer (IE) Security Update 2699988.

The installed version of IE is affected by several vulnerabilities that could allow an attacker to execute arbitrary code on the remote host.

Solution: Microsoft has released a set of patches for XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-037

See Also: http://www.nessus.org/u?c7d49512
http://www.nessus.org/u?18c6adba
http://www.zerodayinitiative.com/advisories/ZDI-12-093/
http://www.securityfocus.com/archive/1/523185/30/0/threaded
http://www.securityfocus.com/archive/1/523186/30/0/threaded
http://www.securityfocus.com/archive/1/523196/30/0/threaded

Risk Factor: High

STIG Severity: II

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

Plugin Output:
The host is missing KB 2699988 according to WSUS.

CPE: cpe:/a:microsoft:internet_explorer
cpe:/o:microsoft:windows

CVE: CVE-2012-1523, CVE-2012-1858, CVE-2012-1872, CVE-2012-1873, CVE-2012-1874, CVE-2012-1875, CVE-2012-1876, CVE-2012-1877, CVE-2012-1878, CVE-2012-1879, CVE-2012-1880, CVE-2012-1881, CVE-2012-1882

BID: 53841, 53842, 53843, 53844, 53845, 53847, 53848, 53866, 53867, 53868, 53869, 53870, 53871

Crossref: OSVDB #82860, OSVDB #82861, OSVDB #82862, OSVDB #82863, OSVDB #82864, OSVDB #82865, OSVDB #82866, OSVDB #82867, OSVDB #82868, OSVDB #82869, OSVDB #82870, OSVDB #82871, OSVDB #82872, EDB-ID #19777, IAVB #2012-B-0066, EDB-ID #20174, MSFT #MS12-037

Vulnerability Publication Date: 2012/06/12

Patch Publication Date: 2012/06/12

Plugin Publication Date: 2012/06/13

Plugin Modification Date: 2012/08/18

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-037.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks: Metasploit (Microsoft Internet Explorer Fixed Table Col Span Heap Overflow)

Plugin	Plugin Name	Severity	Family	Exploit?
59456	MS12-038: Vulnerability in .NET Framework Could Allow Remote Code Execution (2706726)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The .NET Framework installed on the remote Windows host could allow arbitrary code execution.

Description: The version of the .NET Framework installed on the remote host is affected by a code execution vulnerability due to the improper execution of a function pointer.

A remote, unauthenticated attacker could execute arbitrary code on the remote host subject to the privileges of the user running the affected application.

Solution: Microsoft has released a set of patches for .NET Framework 2.0, 3.5, and 4 :

http://technet.microsoft.com/en-us/security/Bulletin/MS12-038

See Also: http://www.zerodayinitiative.com/advisories/ZDI-12-141/
http://www.securityfocus.com/archive/1/523936/30/0/threaded

Risk Factor: High

STIG Severity: II

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 6.9

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:
The host is missing KB 2686831 according to WSUS.

CPE: cpe:/o:microsoft:windows
cpe:/a:microsoft:.net_framework

CVE: CVE-2012-1855

BID: 53861

Crossref: OSVDB #82859, MSFT #MS12-038, IAVA #2012-A-0091

Vulnerability Publication Date: 2012/06/12

Patch Publication Date: 2012/06/12

Plugin Publication Date: 2012/06/13

Plugin Modification Date: 2012/08/20

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: local

Source File: smb_nt_ms12-038.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
59460	MS12-042: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2711167)	High	Windows : Microsoft Bulletins	Yes

Synopsis: The Windows kernel is affected by a multiple vulnerabilities that could result in privilege escalation.

Description: The remote host is running a Windows kernel version that is affected by multiple privilege escalation vulnerabilities:

- A vulnerability exists in the way that the Windows User Mode Scheduler handles system requests that can be exploited to execute arbitrary code in kernel mode. (CVE-2012-0217)

- A vulnerability exists in the way that Windows handles BIOS memory that can be exploited to execute arbitrary code in kernel mode. (CVE-2012-1515)

Solution: Microsoft has released a set of patches for 32-bit versions of Windows XP and 2003 as well as patches for 64-bit versions of Windows 7 and Server 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/MS12-042

Risk Factor: High

STIG Severity: I

CVSS Base Score: 7.2

CVSS Vector: CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 5.3

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:
The host is missing KB 2709715 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-0217, CVE-2012-1515

BID: 52820, 53856

Crossref: OSVDB #82849, OSVDB #82850, MSFT #MS12-042, IAVA #2012-A-0055

Vulnerability Publication Date: 2012/03/19

Patch Publication Date: 2012/06/12

Plugin Publication Date: 2012/06/13

Plugin Modification Date: 2012/06/17

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: local

Source File: smb_nt_ms12-042.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
59906	MS12-043: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)	High	Windows : Microsoft Bulletins	Yes

Synopsis: Arbitrary code can be executed on the remote host through Microsoft XML Core Services.

Description: The version of Microsoft XML Core Services installed on the remote Windows host is affected by a remote code execution vulnerability that could allow arbitrary code execution if a user views a specially crafted web page using Internet Explorer.

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-043

Risk Factor: High

STIG Severity: I

CVSS Base Score: 9.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.4

CVSS Temporal Vector: CVSS2#E:F/RL:W/RC:C

Plugin Output:
The host is missing KB 2719985 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-1889

BID: 53934

Crossref: OSVDB #82873, MSFT #MS12-043, IAVA #2012-A-0111

Vulnerability Publication Date: 2012/07/10

Patch Publication Date: 2012/07/10

Plugin Publication Date: 2012/07/11

Plugin Modification Date: 2012/08/16

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-043.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks: Metasploit (MS12-043 Microsoft XML Core Services MSXML Uninitialized Memory Corruption)

Plugin	Plugin Name	Severity	Family	Exploit?
59912	MS12-049: Vulnerability in TLS Could Allow Information Disclosure (2655992)	Medium	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host has an information disclosure vulnerability.

Description: A design flaw in the CBC mode of operation on the TLS protocol can allow encrypted TLS traffic to be decrypted. This vulnerability could allow for the decryption of HTTPS traffic by an unauthorized third party.

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/MS12-049

Risk Factor: Medium

STIG Severity: II

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2655992 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-1870

BID: 54304

Crossref: OSVDB #83660, MSFT #MS12-049, IAVA #2012-A-0108

Vulnerability Publication Date: 2012/07/10

Patch Publication Date: 2012/07/10

Plugin Publication Date: 2012/07/11

Plugin Modification Date: 2012/07/14

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-049.nasl

First Discovered: Aug 23, 2012 20:38:06 CDT

Last Observed: Aug 23, 2012 20:38:06 CDT

Exploit Frameworks:

Plugin	Plugin Name	Severity	Family	Exploit?
61529	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	Windows : Microsoft Bulletins	Yes

Synopsis: The remote Windows host is potentially affected by multiple code execution vulnerabilities.

Description: The remote Windows host is potentially affected by the following vulnerabilities :

- A denial of service vulnerability exists in Windows networking components. The vulnerability is due to the service not properly handling specially crafted RAP requests. (CVE-2012-1850)

- A remote code execution vulnerability exists in the Windows Print Spooler service that can allow a remote, unauthenticated attacker to execute arbitrary code on an affected system. (CVE-2012-1851)

- A remote code execution vulnerability exists in the way that Windows networking components handle specially crafted RAP responses.
(CVE-2012-1852, CVE-2012-1853)

Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

http://technet.microsoft.com/en-us/security/bulletin/ms12-054

Risk Factor: Critical

STIG Severity: I

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.3

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The host is missing KB 2712808 according to WSUS.

CPE: cpe:/o:microsoft:windows

CVE: CVE-2012-1850, CVE-2012-1851, CVE-2012-1852, CVE-2012-1853

BID: 54921, 54928, 54931, 54940

Crossref: OSVDB #84598, OSVDB #84599, OSVDB #84600, OSVDB #84601, MSFT #MS12-054, IAVA #2012-A-0137

Vulnerability Publication Date: 2012/08/14

Patch Publication Date: 2012/08/14

Plugin Publication Date: 2012/08/15

Plugin Modification Date: 2012/08/18

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: local

Source File: smb_nt_ms12-054.nasl
First Discovered: Aug 23, 2012 20:38:06 CDT
Last Observed: Aug 23, 2012 20:38:06 CDT
Exploit Frameworks: