Recommended Microsoft Security Updates for Cisco TelePresence Content Server Release 5.3.x

May 30, 2017

This bulletin lists the Microsoft Security Updates that are recommended for installation on the Cisco TelePresence Content Server Release 5.3.x. This bulletin is applicable to all versions of the Content Server with Windows 2003 SP2.

Contents

Installation

For each security update, click the link to go directly to the Microsoft web site and do the following:

1. Read the Microsoft Security Bulletin.
2. Download the Security Update by clicking the link on the Security Bulletin web page for Windows Server 2003 SP2.
3. Install the update by following the procedure provided by Microsoft.

Cisco Systems, Inc.
www.cisco.com

Windows 2003 SP2 Security Updates

Microsoft Knowledge Base Article	Executable File
Windows Kernel Patches for Windows 2003 SP2 for Content Server 5.3.x	
Security update for Microsoft Windows SMB Server(4013389) [Ransomware Fix]	windowsserver2003-kb4012598-x86-custom-enu_f617caf6e7ee6f43abe4b386cb1d26b3318693cf.exe
Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (KB2705219 in KB2733594)	WindowsServer2003-KB2705219-v2-x86-ENU.exe
Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (KB2712808 in KB2733594)	WindowsServer2003-KB2712808-x86-ENU.exe
Vulnerabilities in Windows Shell Could Allow Remote Code Execution (KB2727528)	WindowsServer2003-KB2727528-x86-ENU.exe
Vulnerability in Media Decompression Could Allow Remote Code Execution (KB2780091)	WindowsServer2003-KB2780091-x86-ENU.exe
Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution (KB2803821 in KB2847883)	WindowsServer2003-KB2803821-v2-x86-ENU (1).exe
Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (KB2845187)	WindowsServer2003-KB2845187-x86-ENU.exe
Vulnerability in Digital Signatures Could Allow Denial of Service (KB2868626)	WindowsServer2003-KB2868626-x86-ENU.exe
Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege (KB2876315)	WindowsServer2003-KB2876315-x86-ENU.exe
Vulnerability in Windows Kernel Could Allow Elevation of Privilege (KB2914368)	WindowsServer2003-KB2914368-x86-ENU.exe
Vulnerability in LRPC Client Could Allow Elevation of Privilege (KB2898715)	WindowsServer2003-KB2898715-x86-ENU.exe
Vulnerability in Windows Could Allow Remote Code Execution (KB2893294)	WindowsServer2003-KB2893294-x86-ENU.exe
Vulnerability in Windows Graphics Device Interface Could Allow Remote Code Execution (KB2876331)	WindowsServer2003-KB2876331-x86-ENU.exe
Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution (KB2850869)	WindowsServer2003-KB2850869-x86-ENU.exe
Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (KB2820917)	WindowsServer2003-KB2820917-x86-ENU.exe
Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (KB2758857)	WindowsServer2003-KB2758857-x86-ENU.exe

Microsoft Knowledge Base Article	Executable File
Vulnerability in TLS Could Allow Information Disclosure (KB2655992)	WindowsServer2003-KB2655992-x86-ENU.exe
Vulnerability in Windows Shell Could Allow Remote Code Execution (KB2691442)	WindowsServer2003-KB2691442-x86-ENU.exe
Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (KB2929961)	WindowsServer2003-KB2929961-x86-ENU
Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (KB2930275)	WindowsServer2003-KB2930275-x86-ENU
Vulnerability in Security Account Manager Remote (SAMR) Protocol Could Allow Security Feature Bypass (KB2934418)	WindowsServer2003-KB2923392-x86-ENU
Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (KB2922229)	WindowsServer2003-KB2922229-x86-ENU
Vulnerability in Windows Shell Handler Could Allow Elevation of Privilege (KB2962488)	WindowsServer2003-KB2926765-x86-ENU.exe
Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (KB2967487)	WindowsServer2003-KB2957503-x86-ENU.exe
Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (KB2967487)	WindowsServer2003-KB2957509-x86-ENU.exe
Vulnerability in Ancillary Function Driver (AFD) Could Allow Elevation of Privilege (KB2975684)	WindowsServer2003-KB2961072-x86-ENU.exe
Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege (KB2984615)	WindowsServer2003-KB2993651-x86-ENU.exe
Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (KB3000061)	WindowsServer2003-KB3000061-x86-ENU.exe
Vulnerability in Message Queuing Service Could Allow Elevation of Privilege (KB2993254)	WindowsServer2003-KB2993254-x86-ENU.exe
Vulnerability in FAT32 Disk Partition Driver Could Allow Elevation of Privilege (KB2998579)	WindowsServer2003-KB2998579-x86-ENU.exe
Vulnerabilities in Windows OLE Could Allow Remote Code Execution (KB3011443)	WindowsServer2003-KB3006226-x86-ENU.exe
Vulnerability in Schannel Could Allow Remote Code Execution (KB2992611)	WindowsServer2003-KB2992611-x86-ENU.exe
Vulnerability in Kerberos Could Allow Elevation of Privilege (KB3011780)	WindowsServer2003-KB3011780-x86-ENU.exe
Vulnerability in TCP/IP Could Allow Elevation of Privilege (KB2989935)	WindowsServer2003-KB2989935-x86-ENU.exe

Microsoft Knowledge Base Article	Executable File
Vulnerability in Kernel-Mode Driver Could Allow Denial of Service (KB3002885)	WindowsServer2003-KB3002885-x86-ENU.exe
Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (KB3013126	WindowsServer2003-KB3013126-x86-ENU.exe
Vulnerability in Windows Telnet Service Could Allow Remote Code Execution (KB3020393)	WindowsServer2003-KB3020393-x86-ENU.exe
Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege (KB3021674)	WindowsServer2003-KB3021674-x86-ENU.exe
Vulnerability in Network Policy Server RADIUS Implementation Could Cause Denial of Service (KB3014029)	WindowsServer2003-KB3014029-x86-ENU.exe
Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (KB3019215)	WindowsServer2003-KB3019215-x86-ENU.exe
Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (KB3036220)	WindowsServer2003-KB3013455-x86-ENU.exe WindowsServer2003-KB3037639-x86-ENU.exe
Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (KB3036220)	WindowsServer2003-KB3023562-x86-ENU.exe
Vulnerability in Group Policy Could Allow Security Feature Bypass (KB3004361)	WindowsServer2003-KB3004361-x86-ENU.exe
Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (KB3029944)	WindowsServer2003-KB3029944-x86-ENU.exe
Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution (KB3041836)	WindowsServer2003-KB3033889-x86-ENU.exe
Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution (KB3041836)	WindowsServer2003-KB3039066-x86-ENU.exe
Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege (KB3034344)	WindowsServer2003-KB3034344-x86-ENU.exe
Vulnerability in PNG Processing Could Allow Information Disclosure (KB3035132)	WindowsServer2003-KB3035132-x86-ENU.exe
Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (KB3038680)	WindowsServer2003-KB3033395-v2-x86-ENU.exe
Vulnerability in NETLOGON Could Allow Spoofing (KB3002657)	WindowsServer2003-KB3002657-v2-x86-ENU.exe
Vulnerability in Schannel Could Allow Security Feature Bypass (KB3046049)	WindowsServer2003-KB3046049-x86-ENU.exe
Vulnerability in Microsoft Graphics Component Could Allow Remote Code Execution (KB3046306)	WindowsServer2003-KB3046306-x86-ENU.exe

Microsoft Knowledge Base Article	Executable File
Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (KB3049576)	WindowsServer2003-KB3045685-x86-ENU.exe
Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (KB3049576)	WindowsServer2003-KB3045999-x86-ENU.exe
Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (KB3057110)	WindowsServer2003-KB3045171-x86-ENU.exe
Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (KB3057191)	WindowsServer2003-KB3045171-x86-ENU.exe
Vulnerability in Schannel Could Allow Information Disclosure (KB3061518)	WindowsServer2003-KB3061518-x86-ENU.exe
Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (KB3057839)	WindowsServer2003-KB3057839-x86-ENU.exe
Vulnerabilities in Windows Could Allow Remote Code Execution (KB3072631)	WindowsServer2003-KB3067903-x86-ENU.exe
Vulnerability in Netlogon Could Allow Elevation of Privilege (KB3068457)	WindowsServer2003-KB3068457-x86-ENU.exe
Vulnerability in Windows Graphics Component Could Allow Elevation of Privilege (KB3069392)	WindowsServer2003-KB3069392-x86-ENU.exe
Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (KB3070102)	WindowsServer2003-KB3070102-x86-ENU.exe
Vulnerability in Windows Installer Service Could Allow Elevation of Privilege (KB3072630)	WindowsServer2003-KB3072630-x86-ENU.exe
Vulnerabilities in OLE Could Allow Elevation of Privilege (KB3072633)	WindowsServer2003-KB3072633-x86-ENU.exe
Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege (KB3067505)	WindowsServer2003-KB3067505-x86-ENU.exe
Vulnerability in ATM Font Driver Could Allow Elevation of Privilege (KB3077657)	WindowsServer2003-KB3077657-x86-ENU.exe
Category 2: Windows Patches for Application Server for Content Server 5.3.x	
Vulnerability in the Microsoft XML Editor Could Allow Information Disclosure (KB2494113 in KB2543893)	SQLServer2005-KB2494113-x86-ENU
Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure (KB2916036)	WindowsServer2003-KB2916036-x86-ENU
Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure (KB2966061)	WindowsServer2003-KB2939576-x86-ENU.exe

Microsoft Knowledge Base Article	Executable File
Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure (KB2966061)	msxml6-KB2957482-enu-x86.exe
Vulnerability in XML Core Services Could Allow Remote Code Execution (KB2993958)	WindowsServer2003-KB2993958-x86-ENU.exe
Vulnerability in XML Core Services Could Allow Security Feature Bypass (KB3046482)	WindowsServer2003-KB3046482-x86-ENU.exe
Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure (KB2966061)	WindowsServer2003-KB2939576-x86-ENU.exe
Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure (KB2966061)	msxml6-KB2957482-enu-x86.exe
Vulnerability in XML Core Services Could Allow Remote Code Execution (KB2993958)	WindowsServer2003-KB2993958-x86-ENU.exe
Vulnerability in XML Core Services Could Allow Security Feature Bypass (KB3046482)	WindowsServer2003-KB3046482-x86-ENU.exe
Category 3: Windows Patches for Windows Applications and Framework for Content Server 5.3.x	
Vulnerabilities in .NET Framework Could Allow Remote Code Execution (KB2878890)	
.NET framework 2.0 (KB2863239)	NDP20SP2-KB2863239-x86.exe
.NET framework 4.0 (KB2858302-v2)	NDP40-KB2858302-v2-x86.exe
Vulnerability in .NET Framework Could Allow Elevation of Privilege (KB2800277)	
.NET framework 2.0 (KB2789643)	NDP20SP2-KB2789643-x86.exe
.NET framework 4.0 (KB2789642)	NDP40-KB2789642-x86.exe
Vulnerability in Open Data Protocol Could Allow Denial of Service (KB2769327 in KB2736428)	NDP40-KB2736428-x86.exe
Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (KB2916607)	NDP20SP2-KB2901111-x86 NDP20SP2-KB2898856-x86 NDP40-KB2898855-v2-x86 NDP40-KB2901110-v2-x86
Vulnerability in .NET Framework Could Allow Elevation of Privilege (KB2958732)	NDP20SP2-KB2932079-x86.exe
Vulnerability in .NET Framework Could Allow Elevation of Privilege (KB2958732)	NDP40-KB2931365-x86.exe
Vulnerability in .NET Framework Could Allow Denial of Service (KB2990931)	NDP20SP2-KB2972214-x86.exe
Vulnerability in .NET Framework Could Allow Denial of Service (KB2990931)	NDP40-KB2972215-x86.exe

Microsoft Knowledge Base Article	Executable File
Vulnerabilities in .NET Framework Could Allow Remote Code Execution (KB3000414)	NDP20SP2-KB2972105-x86.exe
Vulnerabilities in .NET Framework Could Allow Remote Code Execution (KB3000414)	NDP20SP2-KB2979574-v2-x86.exe
Vulnerabilities in .NET Framework Could Allow Remote Code Execution (KB3000414)	NDP40-KB2972106-x86.exe
Vulnerabilities in .NET Framework Could Allow Remote Code Execution (KB3000414)	NDP40-KB2979575-v2-x86.exe
Vulnerability in .NET Framework Could Allow Elevation of Privilege (KB3005210)	NDP20SP2-KB2978124-x86.exe
Vulnerability in .NET Framework Could Allow Elevation of Privilege (KB3005210)	NDP40-KB2978125-x86.exe
Vulnerability in .NET Framework Could Allow Information Disclosure (KB3048010)	NDP20SP2-KB3037577-x86.exe
Vulnerability in .NET Framework Could Allow Information Disclosure (KB3048010)	NDP40-KB3037578-x86.exe
Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (KB3057134)	NDP20SP2-KB3023220-x86.exe
Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (KB3057134)	NDP20SP2-KB3035488-x86.exe
Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (KB3057134)	NDP40-KB3023221-x86.exe
Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (KB3057134)	NDP40-KB3032662-x86.exe

Not supported for Content Server Release 5.3.x:

- Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (KB2828223)
- Vulnerability in Windows Common Controls Could Allow Remote Code Execution (KB2726929 and KB2687441 in KB2720573)
- Vulnerability in SQL Server Could Allow Elevation of Privilege (KB2716427, KB2716429, and KB2716440 in KB2754849)
- Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution (KB2845142 in KB2847883)

Patches that Resolve Nessus-Identified Vulnerabilities

Nessus is a vulnerability scanner developed by Tenable Network Security. The scanner produces vulnerability checks called *plugins* which are sometimes resolved by Microsoft patches. The recommended Microsoft patches for the Content Server are listed below.

Plugin ID	Description	Executable File/Resolution
20007 Severity Level: Medium	SSL Version 2 (v2) Protocol Detection.	Microsoft provided fix-it 50495 for Windows Server 2003. Or, run the script for Windows Server 2003. See the Release 5.3.2 script for Nessus Plugin Patches on Cisco.com.
45411 Severity Level: Medium	SSL Certificate with wrong Hostname.	The Content Server needs to use a publicly signed certificate instead of the default self-signed certificate. For more information, see the *Cisco TelePresence Content Server Administrator Guide*.
48762 Severity Level: High	Insecure Library Loading could allow Remote Code Execution.	http://technet.microsoft.com/en-us/security/advisory/2269637 **See the "Plugin 48762" section for the executables.**
51192 Severity Level: Medium	SSL Certificate cannot be trusted.	Obtain a publicly signed certificate instead of the default certificate. For more information, see the *Cisco TelePresence Content Server Administrator Guide*.
53382 Severity Level: High	Microsoft Foundation Class Library could allow Remote code execution.	Patch not recommended. Might cause error on installation or uninstallation of the Content Server.
55129 Severity Level: Medium	Microsoft XML editor could allow Information Disclosure.	SQLServer2005-KB2494113-x86-ENU
57582 Severity Level: Medium	SSL Self Signed Certificate.	Obtain a publicly signed certificate instead of the default certificate. For more information, see the *Cisco TelePresence Content Server Administrator Guide*.
57608 Severity Level: Medium	SMB signing required.	Review the supporting information about the issue. Run the script to resolve the issue. See the Release 5.3.2 script for Nessus Plugin Patches on Cisco.com.

Plugin ID	Description	Executable File/Resolution
63155 Severity Level: High	Microsoft Windows Unquoted Service Path Enumerator.	Run the script to resolve the issue. See the Release 5.3.2 script for Nessus Plugin Patches on Cisco.com.
71323 Severity Level: High	Insecure ASP.Net Site Configuration could allow Elevation of Privilege.	Microsoft Security Advisory 2905247 NDP20SP2-KB2894843-x86.exe NDP40-KB2894842-x86.exe

Plugin 48762

These are the executables for addressing Plugin 48762.

Note Before installing patches, execute script and fixit.

Microsoft Knowledge Base Article	Executable File
A new CWDIllegalInDll Search registry entry is available to control the Dll search path algorithm	MicrosoftFixit50522 WindowsServer2003-KB2264107-x86-ENU.exe Run the script to resolve the issue. See the Release 5.3.2 script for Nessus Plugin Patches on Cisco.com.
Vulnerabilities in .NET Framework Could Allow Remote Code Execution (KB2745030)	
.Net Framework v2.0-KB2729450	NDP20SP2-KB2729450-x86.exe
.Net Framework v4.0-KB2729449	NDP40-KB2729449-x86.exe
.Net Framework v4.0-KB2737019	NDP40-KB2737019-x86.exe
Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution (KB2623699)	WindowsServer2003-KB2564958-X86-ENU.exe
Vulnerability in Windows Components Could Allow Remote Code Execution (KB2570974)	WindowsServer2003-KB2570947-x86-ENU.exe
Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (KB2483619 in KB2508062)	WindowsServer2003-KB2483619-x86-ENU.exe
Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution (KB2443105)	WindowsServer2003-KB2443105-x86-ENU.exe
Vulnerability in Windows Address Book Could Allow Remote Code Execution (KB2423809)	WindowsServer2003-KB2423089-x86-ENU.exe
Vulnerability in Windows Media Encoder Could Allow Remote Code Execution (KB2447961)	Windows Media Encoder 9x86

Related Documentation

Cisco TelePresence Content Server Documentation

http://www.cisco.com/en/US/products/ps11347/tsd_products_support_series_home.html

Information About Accessibility and Cisco Products

For information about the accessibility of this product, contact the Cisco accessibility team at accessibility@cisco.com.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.