Q & A

Cisco CallManager **Security** Patch Process

Q. What Cisco products follow this security patch process?

A. Cisco CallManager (CCM), Cisco Customer Response Solutions (CRA/CRS), Cisco Personal Assistant (PA), Cisco Emergency Responder (CER), and Cisco Conference Connection (CCC). Using these supported platforms: Cisco Media Convergence Servers (MCS), Cisco Integrated Communications System (ICS-7750 with CallManager installed only), and Cisco-approved, customer-provided Compaq/HPQ and IBM servers.

Q. Microsoft recently changed the classification process for security alerts. How does this affect the Cisco process for re-posting the patches on the Cisco Web site?

A. The new classification process published by Microsoft is posted at:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/rating.asp

The process is currently under review within Cisco as a result of changes at Microsoft. Although the process may remain the same through a special arrangement with Microsoft, there is presently no commitment by Microsoft to extend the former classification method. If Microsoft does not commit to extending the former classification method, a new Cisco policy will be published to update this one.

Q. Can you summarize how Cisco responds to the security hot fixes posted by Microsoft?

A. Cisco closely monitors security bulletins from Microsoft, and based on impact to Cisco CallManager and applications with the same operating system (OS) installation, the fixes are re-posted to Cisco.com at:

http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des

When Microsoft posts a security patch, Cisco determines if the patch affects the following application and OS components in Cisco CallManager and applications that share the same OS installation process:

- Windows 2000 Server (including any Windows component or subcomponent installed by Cisco)
- Internet Information Server (IIS)
- Internet Explorer
- Structured Query Language (SQL)

Relevant patches are tested to verify correct operation with Cisco applications.

Cisco provides several options for customers to manage the deployment of security patches in their environments, based on customer security and change management requirements:

- Patches that Cisco deems critical for Cisco CallManager and voice applications security are tested and posted to Cisco.com within one business day after the Microsoft announcement. For installation of these patches, Cisco assumes that customers

have applied all service packs for the OS and application components in the preceding list, and only addresses the security patches later than the latest recommended service pack.

- Patches that are not critical are posted to Cisco.com twice per month, in the form of a OS Support Patch.

Q. How does Cisco respond to security patches from hardware vendors that affect BIOS or other system components?

A. Cisco acknowledges security alerts from applicable hardware vendors and follows their criticality guidelines. These hardware vendor patches are posted to the same URL on Cisco.com where software patches are posted.

Q. Can you provide more details on how Cisco assesses the security threat associated with a patch posted by Microsoft?

A. Cisco assumes that critical security patches from Microsoft for Intranet Servers pose an immediate risk to Cisco CallManager users, and these patches should be applied as soon as possible. Even if Cisco does not believe that a security patch identified by Microsoft as critical adversely affects CallManager users, Cisco treats the patch as critical.

Important, Moderate, and Low Security patches may affect Cisco CallManager users, but these patches can be applied in a scheduled maintenance window, following testing and release of a roll-up patch by Cisco twice per month.

If a patch has no affect on Cisco CallManager users because it applies to applications not installed on a CallManager server, Cisco does not consider it applicable.

If Microsoft classifies a security patch as important, moderate, or low priority, but Cisco determines that the patch should be considered critical relative to Cisco CallManager security, Cisco treats the patch as critical.

The Cisco Product Security Incident Response Team (PSIRT) is aware of the testing performed by the Cisco CallManager development teams, as it pertains to various patches released by Microsoft and relevant hardware vendors.

Important: Cisco assumes that Cisco CallManager users have not changed the default configuration of the Windows 2000 Server OS, they have not installed additional Microsoft applications or tools not installed by default with CallManager, and they have not installed any nonsupported third-party applications.

Q. Can you provide more details about the Cisco process for re-posting the security patches?

A. For critical security patches, as classified by Microsoft or a third-party vendor, Cisco tests the patches within one business day of notification, and if safe for the Cisco CallManager application, posts the patch on Cisco.com for immediate use. These critical patches are not delivered in a Cisco installation wrapper; rather, they are in the original form provided by Microsoft or another vendor.

For Important, Moderate, and Low Security patches, as classified by Microsoft or a third-party vendor, Cisco wraps these patches into an OS Support Patch along with any Critical patches that were posted individually twice per month. Cisco tests then posts the OS Support Patch on the 1st and 15th of each month. When these days fall on a weekend or holiday, the patch is posted on the next business day after the weekend or holiday. All security patches received within five business days of the 1st and 15th will be deferred to the next test cycle. Any security patches that are obsolete due to a more current patch on Cisco.com will be removed.

Cisco posts a README file to Cisco.com that lists the approved security patches and service packs that have been tested with Cisco CallManager. All security patches re-posted to the Cisco Web site have been tested and are approved for use with CallManager and related voice applications.

Because each security patch requires a reboot of the Cisco CallManager or voice application server, Cisco recommends that the security patches be applied during maintenance windows.

Cisco takes no action for patches that are not applicable to Cisco CallManager or other applicable voice servers.

Q. Does Cisco handle security patches separately from OS service packs?

A. New service packs from Microsoft are tested and included in the O/S upgrade approximately one to two months after Microsoft releases them. This is separate from the security patches that are rolled up in the OS Support Patch twice a month. Both are posted to the same location on Cisco.com:

http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des

Q. How do customers determine what Microsoft hot fixes (patches) have been applied to their Cisco CallManager servers or voice applications that share the same OS installation process?

A. There are a variety of methods for checking the patch status of different OS and application components:

- Most applied patches are listed in the Add/Remove Programs list based on their Microsoft Knowledge Base number. To view this list, click Start → Settings → Control Panel → Add/Remove Programs.
- Internet Explorer patches do not appear in this list. To view the patches that have been applied to Internet Explorer, open it and then click Help → About Internet Explorer, and look at the Update Versions line. The Knowledge Base number is listed for each patch that is installed.
- SQL patches are not listed. To verify whether an SQL patch has been applied, you can open the Query Analyzer and then run Select @@Version. You can match this version number to the one listed in the Microsoft Knowledge Base article for the patch.
- Microsoft also provides a utility called QFECheck. The utility checks a registry key and then verifies that all the binary files are the correct version. This utility will not work for SQL and Internet Explorer patches. Because QFECheck creates a high load on the CPU during the time it is running, Cisco recommends that this utility be run only during a maintenance window. Details for the QFECheck utility are available at:

  http://support.microsoft.com/default.aspx?scid=kb;EN-US;q282784
- In general, the Microsoft Knowledge Base article for the patch lists in detail how to verify that the patch is installed. This usually requires verifying file date/time stamps or version numbers.

Q. Does Cisco support the HotFix Network Checker utility provided by Microsoft?

A. The Microsoft Hot fix Network Checker (HFNetChk) is a command-line security utility provided by Microsoft. It enables administrators to check the patch status of local or remote devices in the network using an Extensible Markup Language (XML) database regularly updated by Microsoft. This utility will scan for patches to Windows 2000, IIS 5.0, SQL 7.0, and Internet Explorer 5.01 and later. More information about this utility is available at:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/hfnetchk.asp

This Microsoft product is supported by Microsoft. Cisco advises the following for customers who use this utility on Cisco CallManager and related voice application servers:

- The HFNetChk utility consumes significant processor resources when running locally on a server. Cisco recommends that this utility be used only during a maintenance window or from a remote server.

- As one aspect of verifying that all applicable security patches are tested, Cisco verifies that the HFNetChk utility, when run in the baseline security standard (*-b*) mode, reports "all baseline security Hot fixes have been applied."
- Customers who run HFNetChk without the -b option may see messages indicating that patches are missing. Cisco does not test and approve patches that are not applicable for the Cisco CallManager servers. The expected results from HFNetChk are listed in the readme for the OS Support Patch.

Q. What sources does Cisco monitor to learn about security alerts relevant to Cisco CallManager and related voice applications?

A. Cisco tracks several industry sources including, but not limited to:

- Microsoft Security Notification

  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp
- SysAdmin, Audit, Network, Security (SANS) Institute Security Alert Consensus for W2K

  http://server2.sans.org/sansnews
- CERT advisories issued by the Computer Emergency Response Team (CERT) of Carnegie Mellon Software Engineering Institute

  http://www.cert.org/contact_cert/certmaillist.html
- Compaq Product Change Notification (PCN)

  https://www33.compaq.com/pcn/about.asp

Q. What information is typically included in the README file associated with a security patch that is posted to Cisco.com?

A. The following sample README file is representative:

Operating System Upgrade Support Patch Version 2000-2-3spG (win-OS-Upgrade.2000-2-3spG.exe)

- Cumulative Severity = Critical
- App = Multiple Applications
- Description = Post OS Upgrade 2000-2-3 Support Patch
- Install time: < 10 Min.
- Reboot required: Yes
- Dependences: OS version 2000-2-3 or win-OS-Upgrade.2000-2-3.exe
- Replaces previously posted files: win-OS-Upgrade.2000-2-3spF.exe
- New Hot fixes in this release: MS02-068, MS02-069, MS02-070, MS02-071

This upgrade supports all versions of Cisco CallManager (CCM) and all compatible versions of Cisco Customer Response Solutions (CRA/CRS), Cisco Personal Assistant (PA), Cisco Emergency Responder (CER), and Cisco Conference Connection (CCC). Apply this upgrade applies to all Cisco Media Convergence Servers (MCS), Cisco Integrated Communications System (ICS-7750 with CallManager installed only), and Cisco-approved, customer-provided Compaq/HPQ and IBM servers.

Apply this security update to all servers in your cluster.

***This install disrupts call-processing service and requires a reboot. Close all programs before proceeding.*

1. Download the file to a place you will remember.
2. Stop all virus scanning software or Intrusion Detect Software prior to running this installation.
3. Double click on the executable.
4. If the server is on OS version 2000-2-3 or OS upgrade version 2000-2-3 and you are not installing the patches through Terminal Services, answer Yes to the question. If not, install OS Upgrade version 2000-2-3, if needed, and then restart this roll-up from the console.
5. Files extract and then install on the server.
6. Click Yes when prompted and the server reboots.

Note: This support patch will clean up the working directories of the previous OS support patches and copy the log files to C:\Program Files\Common Files\Cisco\Logs.

This support patch includes the following Hot fixes:

Bulletin	Knowledge Base Article	Description	1st Released in Support Patch:
MS01-022	Q296441	WebDAV Service Provider Can Allow Scripts to Levy requests as a User	2000-1-3spA
MS02-008	Q318203	XMLHTTP Control Can Allow Access to Local Files	2000-1-3spF
MS02-009	Q318089	Incorrect VBScript Handling in IE Can Allow Web Pages to Read Local Files	2000-1-3spA
MS02-032	Q320920	26 June 2002 Cumulative Patch for Windows Media Player (version 2)	2000-1-3spE
MS02-042	Q326886	Flaw in Network Connection Manager Could Enable Privilege Elevation	2000-1-3spF
MS02-045	Q326830	Unchecked Buffer in Network Share Provider Can Lead to Denial of Service	2000-1-3spF
MS02-048	Q323172	Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates	2000-1-3spF
MS02-050	Q329115	Certificate Validation Flaw Could Enable Identity Spoofing (version 4)	2000-2-3spA
MS02-051	Q324380	Cryptographic Flaw in RDP Protocol Can Lead to Information Disclosure	2000-2-3spB
	Q327752	Some Winsock API May Cause High CPU Load	2000-2-3spB
MS02-055	Q323255	Unchecked Buffer in Windows Help Facility Could Enable Code Execution	2000-2-3spC
MS02-058	Q328676	Unchecked Buffer in Outlook Express S/MIME Parsing Could Enable System Compromise	2000-2-3spD
MS02-062	Q327696	Cumulative Patch for Internet Information Service	2000-2-3spE

Bulletin	Knowledge Base Article	Description	1st Released in Support Patch:
MS02-063	Q329834	Unchecked Buffer in PPTP Implementation Could Enable Denial of Service Attacks	2000-2-3spE
MS02-065	Q329414	Buffer Overrun in Microsoft Data Access Components Could Lead to Code Execution	2000-2-3spF
MS02-068	Q324929	Cumulative Patch for Internet Explorer	2000-2-3spG
MS02-069	Q810030	Flaw in Microsoft VM Could Enable System Compromise	2000-2-3spG
MS02-070	Q329170	Flaw in SMB Signing Could Enable Group Policy to be Modified	2000-2-3spG
MS02-071	Q328310	Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation	2000-2-3spG

Verifying Hot fixes are installed:

HFNetChk

You can download HFNetChk, a utility provided by Microsoft to scan computers for missing hot fixes and service packs, from Microsoft's Web site. If you run HFNetChk, some hot fixes have not, and should not, be installed. Listed below are the expected results from HFNetChk on a fully patched system:

Bulletin	Knowledge Base Article	Message	Reason
MS01-022	Q296441	Note	This Hot fix should be installed. See Microsoft Knowledge Base Article Q306460 explanation.
MS02-008	Q318202, Q318203, Q317244	Note	This Hot fix should be installed. See Microsoft Knowledge Base Article Q306460 explanation.
MS02-035	Q263968	Note	This Hot fix should be installed. See Microsoft Knowledge Base Article Q306460 explanation.
MS02-040	Q326573	Note	This Hot fix should be installed. See Microsoft Knowledge Base Article Q306460 explanation.
MS02-053	Q324096	Note	This Hot fix is for FrontPage Server Extentions, which should not be installed.
MS02-061	Q316333	Note	This Hot fix should be installed. See Microsoft Knowledge Base Article Q306460 explanation.
MS02-064	Q327522	Note	This is not a hot fix, but a permission setting. OS Upgrade 2000-2-3 already corrects this setting. See Microsoft Knowledge Base Article Q306460 explanation.
MS02-065	Q329414	Note	This Hot fix should be installed. See Microsoft Knowledge Base Article Q306460 explanation.

Note: This is the report from HFNetChk v3.41 and XML data version 1.0.1.438 (12/11/2002). Version 3.32 does not correctly report SQL 7.0 SP4.

QFEcheck

QFEcheck, a utility provided by Microsoft, verifies that hot fixes are correctly installed on a server. Previous OS Support Patches and the current OS Upgrade install this utility. It does not report all hot fixes Internet Explorer, Windows Media Player, SQL hot fixes are not reported by this utility.

Expected results from qfecheck.exe on an up-to-date server:

"Current Service Pack Level": Service Pack 3

Hot fixes Identified:

Q282784: Current on system.

Q323172: Current on system.

Q323255: Current on system.

Q324380: Current on system.

Q326830: Current on system.

Q326886: Current on system.

Q327696: Current on system.

Q327752: Current on system.

Q328310: Current on system.

Q329115: Current on system.

Q329170: Current on system.

Q329834: Current on system.

Q810030: Current on system."

Note: You may see more hot fixes on this list, depending on what you previously installed.

Verifying Hot fixes not reported by QFEcheck

MS01-022 Q296441 "WebDAV Service Provider Can Allow Scripts to Levy requests as a User"

Verify this file version is equal or greater than:

Msdaipp.dll 8.103.4004.0

MS02-008 Q318203 "XMLHTTP Control Can Allow Access to Local Files"

Verify this file version is equal or greater than:

Msxml3.dll 8.20.9415.0

MS02-009 Q318089 "Incorrect VBScript Handling in IE can Allow Web Pages to Read Local Files"

Verify this file version is equal or greater than:

Vbscript.dll 5.5.0.7426

MS02-032 Q320920 "26 June 2002 Cumulative Patch for Windows Media Player (version 2)"

Verify these file versions are equal or greater than:

Dxmasf.dll 6.4.09.1121

Msdxm.ocx 6.4.09.1124

MS02-055 Q328676 "Unchecked Buffer in Outlook Express S/MIME Parsing Could Enable System Compromise"

Verify this file version is equal or greater than:

Inetcomm.dll 5.50.4920.2300

Msoe.dll 5.50.4920.2300

MS02-065 Q329414 "Buffer Overrun in Microsoft Data Access Components Can Lead to Code Execution"

Verify these file version are equal or greater than:

Msadce.dll 2.53.6202.0

Msadco.dll 2.53.6202.0

Msadcs.dll 2.53.6202.0

Msdaprst.dll 2.53.6202.0

MS02-066 Q328970 "Cumulative Patch for Internet Explorer"

Run Internet Explorer then click Help | About Internet Explorer

Under "Update Version:" it should list Q324929

Or

Verify these file versions are equal or greater than:

Mshtml.dll 5.50.4922.900

Pngfilt.dll 5.50.4922.900

Shdocvw.dll 5.50.4923.900

url.dll 5.50.4915.500

urlmon.dll 5.50.4922.900

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

SD/LW3871 0103