

Cisco Security Advisory: Cisco IOS HTTP Server Vulnerability

Document ID: 13627

Advisory ID: cisco-sa-20000514-ios-http-server

<http://www.cisco.com/warp/public/707/cisco-sa-20000514-ios-http-server.shtml>

Revision 1.1

Last Updated 2002 March 11 1300 UTC (GMT)

For Public Release 2000 May 14 1300 UTC (GMT)

Please provide your feedback on this document.

- Summary
- Affected Products
- Details
- Impact
- Software Versions and Fixes
- Workarounds
- Obtaining Fixed Software
- Exploitation and Public Announcements
- Status of This Notice: INTERIM
- Distribution
- Revision History
- Cisco Security Procedures

Summary

A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled and browsing to "http://<router-ip>/%%" is attempted. This defect can be exploited to produce a denial of service (DoS) attack. This defect has been discussed on public mailing lists and should be considered public information.

The vulnerability, identified as Cisco bug ID CSCdr36952, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 11.1 through 12.1, inclusive. The vulnerability has been corrected and Cisco is making fixed releases available to replace all affected IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect as shown in detail below.

The vulnerability can be mitigated by disabling the IOS HTTP server, using an access-list on an interface in the path to the router to prevent unauthorized network connections to the HTTP server, or applying an access-class option directly to the HTTP server itself. The IOS HTTP server is enabled by default only on Cisco 1003, 1004, and 1005 routers that are not configured. In all other cases, the IOS http server must be explicitly enabled in order to exploit this defect.

The complete advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20000514-ios-http-server.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The following list of products are affected if they are running a release of Cisco IOS software that has the defect. To determine if a Cisco product is running IOS, log in to the device and issue the command **show version**. Classic Cisco IOS software will identify itself simply as "Internetwork Operating System Software" or "IOS (tm)" software and will display a version number. Other Cisco devices either will not have the **show version** command, or will give different output. Compare the version number obtained from the router with the versions presented in the Software Versions and Fixes section below.

Cisco devices that may be running affected releases include:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800, ubr900, 1000, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200, ubr7200, 7500, and 12000 series.
- Most recent versions of the LS1010 ATM switch.
- The Catalyst 6000 if it is running IOS.
- Some versions of the Catalyst 2900XL and 3500XL LAN switches.
- The Cisco DistributedDirector.

For some products, the affected software releases are relatively new and may not be available on every device listed above.

Products Confirmed Not Vulnerable

If you are not running classic Cisco IOS software then you are not affected by this vulnerability. Cisco products that do not run classic Cisco IOS software and thus are not affected by this defect include:

- 700 series dialup routers (750, 760, and 770 series) are not affected.
- Catalyst 1900, 2800, 2900, 3000, and 5000 series LAN switches are not affected. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, are affected (see the Affected Products section above).
- The Catalyst 6000 is not affected if it is not running IOS.
- WAN switching products in the IGX and BPX lines are not affected.
- The MGX (formerly known as the AXIS shelf) is not affected.
- No host-based software is affected.
- The Cisco PIX Firewall is not affected.
- The Cisco LocalDirector is not affected.
- The Cisco Cache Engine is not affected.

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

The HTTP server was introduced in IOS release 11.0 to extend router management to the worldwide web. The defect appears in a function added in IOS releases 11.1 and 11.2 that parses special characters in a URI of the format "%nn" where each "n" represents a hexadecimal digit. The vulnerability is exposed when an attempt is made to browse to "http://<router-ip>/%%". Due to the defect, the function incorrectly parses "%%" and it enters an infinite loop. A watchdog timer expires two minutes later and forces the router to crash and reload. Once it has resumed normal operation, the router is again vulnerable to the same defect until the HTTP server is disabled, access from untrusted hosts is prohibited, or the router is upgraded to a release of Cisco IOS software that is not vulnerable to this defect.

In rare cases, the affected device fails to reload, forcing the administrator to cycle the power to resume operation. Some devices have reloaded without providing stack traces and may indicate wrongly that they were "restarted by power-on" when that did not occur.

The HTTP server is *not* enabled by default except on unconfigured Cisco model 1003, 1004, and 1005 routers. Once initial access is granted to configure the router, the customer may disable or limit access to the HTTP server by changing the configuration. Once the new configuration has been saved, the the HTTP server will not be enabled automatically when the router restarts.

Impact

Any affected Cisco IOS device that is operating with the HTTP server enabled and is not protected against unauthorized connections can be forced to halt for a period of up to two minutes and then reload. The vulnerability can be exercised repeatedly, possibly creating a denial of service (DoS) attack, until such time as the HTTP server is disabled, the router is protected against the attack, or the software on the router is upgraded to an unaffected release of IOS.

In rare instances when a router at a remote location fails to reload, an administrator must visit the physical device to recover from the defect. In rare cases where no stack trace could be recovered and the router may erroneously report "restarted by power-on", the customer may be misled as to the true cause of a reload.

Software Versions and Fixes

The following table summarizes the major releases of Cisco IOS software affected by the defect described in this notice and scheduled dates on which the earliest corresponding fixed releases will be available. All dates are tentative and subject to change.

Each row of the table shows the earliest release that contains the fix for the vulnerability in the "Rebuild", "Interim", or "Maintenance" columns, presented in release number order.

A Maintenance Release is the most heavily-tested and highly-recommended release in a given row.

A Rebuild Release is constructed from the previous maintenance or mainline release with the addition of a code fix for the specific defect. Although it receives less testing than a maintenance release, it is built from the previous maintenance release and includes only the minimum changes necessary to address the specific defect.

An Interim Release has much less testing than a maintenance release and should be selected only if there is no other suitable release that fixes the defect.

To find an appropriate replacement for a vulnerable release, compare the release number as reported by the **show version** command to the major releases in the first column below. For example, if your device reports that it is running 12.0(5)S, find the row in the table for 12.0S. Reading across to the right, you find that the earliest maintenance release containing the fix will be 12.0(11)S, which will be available for download from CCO on or about 2000-5-29. The earliest interim release containing the fix will be 12.0(10.6)S, available on or about 2000-05-15. The rebuild of the previous maintenance release, 12.0(10)S1, should be available on 2000-05-01.

The only difference between 12.0(10)S and 12.0(10)S1 is the minimum change necessary to fix this vulnerability. In particular, 12.0(10)S1 will not contain any fixes or features applied to any interim releases since the earlier maintenance release, whereas the interim release, 12.0(10.6)S, contains the fix as well as the features and instabilities introduced by previous interim releases, 12.0(10.1)S through 12.0(10.5)S. Therefore, based on this example:

- If you can apply a workaround or otherwise wait for the maintenance release, then upgrade to 12.0(11)S.
- Or
- If you are running 12.0(10.1)S to 12.0(10.5)S inclusive and need some functionality introduced in those interim releases, upgrade to 12.0(10.6)S. Upgrade to 12.0(11)S or later as soon as possible.
- Or
- If you are running release 12.0(10)S or earlier, upgrade to 12.0(10)S1.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that their current hardware and software configurations will continue to be supported properly by the new release.

Major Release	Description or Platform	Availability of Repaired Releases*		
Unaffected Earlier Releases		Rebuild	Interim**	Maintenance
11.0 & earlier, all variants	Numerous	Not vulnerable	Not vulnerable	Not vulnerable
11.1-based Releases		Rebuild	Interim**	Maintenance
11.1	General Deployment (GD): all platforms	Unavailable	Unavailable	Unavailable
11.1CA	Core/ISP support: rsp, c7200		11.1(33.2)CA	11.1(34)CA
11.1CC	FIB support: rsp, c7200	11.1(33)CC1	2000-05-08 11.1(33.1)CC	2000-05-30 11.1(34)CC
		2000-05-10	2000-05-22	2000-06-12
11.2-based Releases		Rebuild	Interim**	Maintenance
11.2	General Deployment (GD): all platforms	11.2(22a)	11.2(22.2)	11.2(23)
		2000-05-29	2000-05-08	2000-07-10

11.2BC	IBM networking, CIP & TN3270 support: rsp	11.2(22a)BC	11.2(22.1)BC	
11.2P	All platforms	2000-05-31 11.2(22a)P	2000-05-05 11.2(22.2)P	11.2(23)P
		2000-05-29	2000-05-08	2000-07-17
11.3-based Releases		Rebuild	Interim**	Maintenance
11.3DA	xDSL access multiplexer: c6200	11.3(1)DA9		
12.0-based Releases		Rebuild	Interim**	Maintenance
12.0	General Deployment (GD): all platforms	12.0(11a)	12.0(11.1)	12.0(12)
12.0DA	xDSL support: 6100, 6200	2000-05-31 12.0(8)DA5	2000-05-22	2000-07-17
		2000-05-31		
12.0S	Core/ISP support: gsr, rsp, c7200	12.0(10)S1	12.0(10.6)S	12.0(11)S
12.0SC	Cable/broadband ISP:ubr7200	2000-05-03	2000-05-15 12.0(10.6)SC	2000-05-29 12.0(11)SC
			2000-05-15	2000-05-30
12.0SL	10000 ESR: c10k	12.0(9)SL1		12.0(10)SL
		2000-05-15		2000-05-31
12.0ST	MPLS/VPN support: gsr, rsp, c7200	12.0(9)ST1		12.0(10)ST
12.0W5	cat8510c, cat8540c, c6msm	2000-05-31		2000-06-12 12.0(5)W5(13d)
	ls1010, cat8510m, cat8540m			2000-05-19 12.0(7)W5(15c)
	cat2948g, cat4232			2000-05-08 12.0(7)W5(15d)
	c5atm, c5atm, c3620, c3640, c4500, c5rsfc, c5rsm, c7200, rsp			2000-05-12 12.0(9)W5(17a)
12.0WC	2900x1, 3500x1			2000-05-22 12.0(5.4)WC1
12.1-based Releases		Rebuild	Interim**	Maintenance

12.1	General Deployment (GD) candidate: all platforms	12.1(1b)	12.1(2.1)	12.1(3)
12.1AA	Access & Dial Early Deployment (ED): c5200, c5300, c5800, dsc-c5800	2000-05-01 12.1(1)AA2	2000-05-15	2000-07-10 12.1(2)AA
12.1DA	xDSL support: 6160, 6260	2000-05-31		2000-05-22 12.1(1)DA
				2000-05-11
12.1DB	xDSL support: c6400			12.1(1)DB
				2000-05-30
12.1DC	xDSL NRP support: c6400r			12.1(1)DC
				2000-05-15
12.1E	ELB Early Deployment (ED): cat6k, 8500, ls1010, 7500, 7200, 7100	12.1(1)E2		12.1(2)E
12.1EC	Cable/broadband Early Deployment (ED): ubr7200	2000-05-04		2000-05-30 12.1(2)EC
12.1T	New technology Early Deployment (ED): all platforms		12.1(2.0.1)T2	2000-05-30 12.1(2)T
12.1XZ***	Obsolete	12.1(1)XA3	2000-05-01	2000-05-22 12.1(2)T***
		2000-05-31		2000-05-22
12.1XD	Early Deployment (ED): limited platforms			12.1(1)XD
12.1XE	Early Deployment (ED): limited platforms			2000-05-15 12.1(1)XE
Notes				2000-05-08
* All dates are estimated and subject to change.				

** Interim releases are subjected to less rigorous testing than regular maintenance releases, and may have serious bugs.

*** 12.1XA is obsolete. Customers should upgrade to 12.1(2)T when it becomes available. This is not a misprint.

Workarounds

In lieu of an upgrade, the threat may be eliminated or reduced by any of the following measures:

- Completely disable the HTTP server using the command **no ip http server** while in global configuration mode.
Or
- If the HTTP server must remain enabled while unrepaired, network access to it can be controlled by applying a standard access list to the HTTP service itself. For example, if the router's HTTP service should be reachable only from a browser running on a computer at IP address 10.1.2.3, then use the following commands in global configuration mode to create a standard access list and apply it to the HTTP server:
access-list 1 permit 10.1.2.3
ip http access-class 1
If access list 1 is already in use, then choose another number in the range 0–99. The implicit deny rule added to the end of every access list will prevent access from any other IP addresses.
Or
- Prevent network access to a vulnerable HTTP server by blocking traffic in the network path to the server's port with an extended access list. Such a list would be applied on an interface of the vulnerable router itself or on another Cisco router in the path of a potential attack, e.g., applied inbound on the outside interface of an edge router. The port number used in the extended access list statement must be the default port used by the HTTP server, port 80, or equal to whatever value it may have been set via the **ip http port** command. Please use this particular workaround with great care; it cannot be recommended confidently without knowledge of specific customer network configurations.

Be sure to save the resulting configuration in memory so that protection of the server is not inadvertently removed after a reload.

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

This vulnerability was announced on the BUGTRAQ mailing list on 2000-04-27 with sufficient information that anyone could exercise the flaw. The Cisco PSIRT responded the same day and acknowledged the vulnerability in e-mail to the BUGTRAQ list with preliminary information regarding estimates of affected platforms and releases as well as a workaround to mitigate the threat. Following the response to BUGTRAQ, the Cisco PSIRT sent a preliminary warning with similar content to cust-security-announce@cisco.com and several internal Cisco mailing lists.

This vulnerability has been discussed in detail on full-disclosure mailing lists and web sites, and requires no special equipment to be exploited.

The Cisco PSIRT has received no reports of malicious exploitation of this vulnerability.

Status of This Notice: INTERIM

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

This notice will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20000514-ios-http-server.shtml>. In addition to this HTML version on Cisco's Worldwide Web site, a text version of this notice will be clear-signed with the Cisco PSIRT PGP key and posted to the following e-mail addresses and Usenet newsgroups:

- cust-security-announce@cisco.com
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- Various internal Cisco mailing lists

Future updates of this notice, if any, will be placed on Cisco's Worldwide Web server, and may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the URL given above for any updates.

Revision History

Revision 1.1	2002-March-11	Updates made to Affected Products and Software Versions and Fixes.
Revision 1.0	2000-May-14	Initial public release.

Cisco Security Procedures

The web page at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html describes how to report security vulnerabilities in Cisco products, obtain assistance with security incidents, and register to receive product security information from Cisco Systems, Inc., including instructions for press inquiries regarding Cisco Security Advisories and notices. This advisory is Cisco's official public statement regarding this vulnerability.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

