

Cisco Security Advisory: Cisco IOS HTTP Server Query Vulnerability

Document ID: 13628

Advisory ID: cisco-sa-20001025-ios-http-server-query

<http://www.cisco.com/warp/public/707/cisco-sa-20001025-ios-http-server-query>

Revision 1.6

Last Updated 2006 March 17 1900 UTC (GMT)

For Public Release 2000 October 25 1600 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: FINAL](#)
[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, browsing to "http://router-ip/anytext?/" is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.

The vulnerability, identified as Cisco bug ID **CSCdr91706**, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 12.0 through 12.1, inclusive. This is **not** the same defect as **CSCdr36952**.

The vulnerability has been corrected and Cisco is making fixed releases available for free 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.

This vulnerability can only be exploited if the enable password is known or not set.

The complete advisory is available at
<http://www.cisco.com/warp/public/707/cisco-sa-20001025-ios-http-server-query.shtml>.

Cisco Security Advisory: Cisco IOS HTTP Server Query Vulnerability

Affected Products

This section provides details on affected products.

Vulnerable Products

The following products are affected if they run a Cisco IOS software release that has the defect. To determine if a Cisco product is running an affected IOS, log in to the device and issue the command **show version**. Cisco IOS software will identify itself as "**Internetwork Operating System Software**" or "**IOS (tm)**" software and will display a version number. Other Cisco devices either will not have the command **show version**, 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 with affected IOS software releases include:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800, ubr900, 1000, 1400, 1500, 1600, 1700, 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.
- The Catalyst 2900XL LAN switch only if it is running IOS.
- The Catalyst 1900, 2800, 2900, 3000, and 5000 series LAN switches are affected.
- 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 Cisco IOS software, you are not affected by this vulnerability.

Cisco products that do not run Cisco IOS software and are not affected by this defect include, but are not limited to:

- 700 series dialup routers (750, 760, and 770 series) are not affected.
- 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.
- 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 "?" (question mark) character is defined in the HTML specifications as a delimiter for CGI arguments. It is also interpreted by the IOS command-line interface as a request for help.

As of Cisco IOS Software Release 12.0T, the meaning of a question mark when it appears adjacent to a "/" (slash) character cannot be determined properly by the URI parser in affected versions of Cisco IOS software. When a URI containing "?/" is presented to the HTTP service on the router and a valid enable password is supplied, the router enters an infinite loop. A watchdog timer expires two minutes later and forces the router to crash and reload. The router continues to be vulnerable to this defect as long as it is running an affected IOS software release and the enable password is known.

This vulnerability may only be exploited if the enable password is not set, it is well known, or it can be guessed.

In rare cases, an affected device fails to reload, which means an administrator must physically cycle the power to resume operation.

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 set an enable password, and disable or limit access to the HTTP server by changing the configuration. Once the new configuration has been saved, the HTTP server will not be enabled when the router restarts.

The Cisco Bug ID **CSCdr91706** relates to fixes for IOS; the fixes for the affected switch product lines are listed with Cisco Bug ID **CSCds57774** and **CSCdv38391**.

Impact

An affected Cisco IOS device that is operating with the HTTP service enabled and is not protected by having the enable password configured can be forced to halt for up to two minutes and then reload. The vulnerability can be exercised repeatedly, possibly creating a denial of service (DOS) attack, unless the service is disabled, the enable password is set, or the router is upgraded to a fixed release.

In instances in which a router at a remote location fails to reload, an administrator must visit the site to enable the device to recover from the defect.

Software Versions and Fixes

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

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

A Maintenance Release is the most heavily tested and highly recommended release.

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

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

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that 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	11.1 AA, 11.1 CA, 11.1 CC, 11.1 CT, 11.1 IA	Not vulnerable	Not vulnerable	Not vulnerable
11.2	11.2 BC, 11.2 P, 11.2 F, 11.2 GS, 11.2 WA3, 11.2 XA	Not vulnerable	Not vulnerable	Not vulnerable
11.3	11.3 NA, 11.3 AA, 11.3 DA, 11.3 XA, 11.3 HA, 11.3 WA, 11.3 MA, 11.3 DB	Not vulnerable	Not vulnerable	Not vulnerable
Pre 12.0-based Releases		Rebuild	Interim**	Maintenance
11.2 SA				
12.0-based Releases		Rebuild	Interim**	Maintenance
12.0	General Deployment (GD): all platforms	Not vulnerable	Not vulnerable	Not vulnerable
12.0DA	xDSL support: 6100, 6200	Not vulnerable	Not vulnerable	Not vulnerable
12.0S	Core/ISP support: gsr, rsp, c7200	Not vulnerable	Not vulnerable	Not vulnerable
12.0SC	Cable/broadband ISP:ubr7200	Not vulnerable	Not vulnerable	Not vulnerable
12.0SL	10000 ESR: c10k	Not vulnerable	Not vulnerable	Not vulnerable
12.0T	Early Deployment(ED): VPN, Distributed director, various platforms			12.1(5)
12.0W5	cat8510c, cat8540c, c6msm ls1010, cat8510m,			2000-OCT-30 12.0(13)W5(19) 2000-NOV-13

	cat8540m c5atm, c5atm, c3620, c3640, c4500, c5rsfc, c5rsm, c7200, rsp			
	cat2948g, cat4232			12.0(10)W5(18e) 2000-NOV-14
12.0XA	Early Deployment (ED): limited platforms			12.1(5)
12.0XE	Early Deployment (ED): limited platforms	12.1(3a)E4		
12.0XH	Early Deployment (ED): limited platforms	2000-OCT-24 12.0(4)XH4		
12.0XJ	Early Deployment (ED): limited platforms	Unknown 12.0(5)XJ6		
12.1-based Releases		Unknown	Rebuild	Interim** Maintenance
12.1	General Deployment (GD) candidate: all platforms			12.1(05)
12.1AA	Access & Dial Early Deployment (ED): c5200, c5300, c5800, dsc-c5800			2000-OCT-30 12.1(5)AA
12.1DA	xDSL support: 6160, 6260			2000-NOV-13 12.01(04)DA
12.1DB	xDSL support: c6400			2000-OCT-30 12.01(4)DB
12.1DC	xDSL NRP support: c6400r			2000-NOV-13 12.01(4)DC
12.1E	ELB Early Deployment (ED): cat6k, 8500, ls1010, 7500, 7200, 7100	12.1(3a)E4		
12.1EC	Cable/broadband Early Deployment (ED): ubr7200	2000-OCT-24 12.01(03a)EC1		

Unknown

12.1T	New technology Early Deployment (ED): all platforms			12.1(5)T
12.1XA	Early Deployment (ED): limited platforms	Not scheduled		2000-NOV-20 12.1(5)T
12.1XB	Early Deployment (ED): limited platforms	Not scheduled		
12.1XC	Early Deployment (ED): limited platforms	Not scheduled		12.1(5)T
12.1XD	Early Deployment (ED): limited platforms	Not scheduled		12.1(5)T
12.1XE	Early Deployment (ED): limited platforms	Not scheduled		12.1(5)T
12.1XF	Early Deployment (ED): limited platforms	12.1(2)XF2		12.1(5)T
12.1XG	Early Deployment (ED): limited platforms	2000-NOV-13 12.1(3)XG2		
12.1XH	Early Deployment (ED): limited platforms	2000-NOV-13 Not scheduled		12.1(5)T
12.1XI	Early Deployment (ED): limited platforms	Not scheduled		
12.1XJ	Early Deployment (ED): limited platforms	Not scheduled		
12.1XL	Early Deployment (ED): limited platforms	Not scheduled		
12.1XP	Early Deployment (ED): limited platforms	12.1(3)XP2		12.1(5)T
Notes		2000-NOV-13		
* 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.				

Workarounds

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

- Select and configure strong enable passwords on networking devices.
Or
- 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 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. Use this workaround with great care; it cannot be recommended confidently without knowledge of specific customer network configurations.

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

The Cisco PSIRT was alerted to this issue by CORE SDI, which discovered the issue during routine security audits on equipment. The security audit included a check for common CGI vulnerabilities against a Cisco device without a configured password; the audit attempted to browse to "http://<router-ip>/cgi-bin/source-help?", which caused the device to crash and reload.

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

Status of This Notice: FINAL

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.

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-20001025-ios-http-server-query.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

Revision History

Revision 1.6	2006-March-17	Changed 12.XC to 12.1XC in the "Software versions and fixes" section; updated Final status text.
Revision 1.5	2003-March-05	Added additional Bug ID's in detail section for other affected hardware.
Revision 1.4	2002-September-25	Updated Status of This Notice section to FINAL.
Revision 1.3	2000-November-01	Updated Affected Products section with "Catalyst 1900, 2800, 2900, 3000, and 5000 series LAN switches are affected." Removed "11.2 SA" from the list of unaffected 11.2 releases. Added "11.2 SA" to pre 12.0-based affected releases. Added availability date and upgrade version for 12.0T. Changed sentence "Select and configure strong passwords on

		networking devices." to "Select and configure strong enable passwords on networking devices."
Revision 1.2	2000–October–26	Updated table info for 12.1 XF, 12.1 XG and 12.1 XP. Added Catalyst 2800 as an affected product in "Affected Products" section.
Revision 1.1	2000–October–25	Updated table info for 12.1T and 12.1AA.
Revision 1.0	2000–October–25	Initial public release.

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

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

Updated: Mar 17, 2006

Document ID: 13628
