

Cisco Security Advisory: IOS HTTP Server Command Injection Vulnerability

Advisory ID: cisco-sa-20051201-http

<http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml>

Revision 1.3

Last Updated 2009 October 22 2000 UTC (GMT)

For Public Release 2005 December 01 2100 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[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 vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a **show buffers** command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

This section provides details on affected products.

☐ Vulnerable Products

This security advisory applies to all Cisco products that run Cisco IOS Software versions 11.0 through 12.4 with the HTTP server enabled. A system which contains the IOS HTTP server or HTTP secure server, but does not have it enabled, is not affected.

To determine if the HTTP server is running on your device, issue the **show ip http server status** and **show ip http server secure status** commands at the prompt and look for output similar to:

```
Router>show ip http server status  
HTTP server status: Enabled
```

If the device is not running the HTTP server, you should see output similar to:

```
Router>show ip http server status  
HTTP server status: Disabled
```

Any version of Cisco IOS prior to the versions which will be listed in the Fixed Software section below may be vulnerable.

☐ Products Confirmed Not Vulnerable

Cisco IOS XR is not affected.

To determine the software running on a Cisco product, log in to the device and issue the **show version** command to display the system banner. Cisco IOS Software will identify itself as "Internetwork Operating System Software" or simply "IOS". On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the **show version** command or will give different output.

The following example identifies a Cisco product running IOS release 12.3(6) with an installed image name of C3640-I-M:

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-I-M), Version 12.3(6),
RELEASE SOFTWARE (fc3)
```

The next example shows a product running IOS release 12.3(11)T3 with an image name of C3845-ADVIPSERVICESK9-M:

```
Cisco IOS Software, 3800 Software (C3845-
ADVIPSERVICESK9-M), Version 12.3(11)T3, RELEASE
SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
```

Additional information about Cisco IOS release naming can be found at <http://www.cisco.com/warp/public/620/1.html>.

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

[Top of the section](#) [Close Section](#)

☐ Details

The Cisco IOS Web browser interface (which enables the device to perform as an HTTP server)

allows configuration and monitoring of a router or access server using any web browser. This feature was introduced in IOS 11.0.

A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a **show buffers** command, will be passed to the browser requesting the page. This HTML code could be interpreted by the browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks.

In order to be vulnerable to the cross-site scripting attack, a user must browse and view the content during the same period of time the injected code exists in memory. On the other hand, if a user does not browse contaminated dynamic content on the device, then exploitation is not possible.

A proof of concept exploit exists for this vulnerability, in which the exploit attempts to reset the enable password on the device. For the attack to work against the device itself, the user browsing tainted dynamic content on the router will only be able to execute commands at or below the privilege level for which they are authenticated and authorized for on the device.

This vulnerability is documented in Cisco Bug ID [CSCsc64976](#) ([registered](#) customers only) .

[Top of the section](#) [Close Section](#)

☐ **Impact**

Successful exploitation of the vulnerability may result in an attacker executing commands on the device, including the possibility of gaining full administrative privileges on the device which is dependent on the privilege level of the authenticated user.

[Top of the section](#) [Close Section](#)

☐ **Software Versions and Fixes**

No software fixes are currently available. This section will be updated regularly as soon as software fixes are available.

[Top of the section](#) [Close Section](#)

☐ **Workarounds**

Disable the HTTP Server

If the HTTP server is not used for any legitimate purposes on the device, it is a best practice to disable it by issuing the following commands in configure mode:

```
no ip http server
no ip http secure-server
```

Disable the HTTP WEB_EXEC Service

A feature was introduced in 12.3(14)T and later in which selective HTTP and HTTPS services could be enabled or disabled. The WEB_EXEC service provides a facility to configure the box and retrieve the current state of the box from remote clients.

It is possible to disable the WEB_EXEC service while still leaving other HTTP services active. If an installation does not require the use of the WEB_EXEC service, then it may be disabled using the following procedure:

1. Verify the list of all session modules.

```
Router#show ip http server session-module
HTTP server application session modules:
  Session module Name  Handle Status  Secure-status
Description
HTTP_IFS                1      Active  Active
HTTP based IOS File Server
HOME_PAGE               2      Active  Active
IOS Homepage Server
QDM                     3      Active  Active
QOS Device Manager Server
QDM_SA                 4      Active  Active
QOS Device Manager Signed Applet Server
WEB_EXEC                5      Active  Active
HTTP based IOS EXEC Server
IXI                     6      Active  Active
IOS XML Infra Application Server
IDCONF                 7      Active  Active
IDCONF HTTP(S) Server
XSM                     8      Active  Active
XML Session Manager
VDM                     9      Active  Active
VPN Device Manager Server
XML_Api                10     Active  Active
XML Api
```

ITS	11	Active	Active
IOS Telephony Service			
ITS_LOCDIR	12	Active	Active
ITS Local Directory Search			
CME_SERVICE_URL	13	Active	Active
CME Service URL			
CME_AUTH_SRV_LOGIN	14	Active	Active
CME Authentication Server			
IPS_SDEE	15	Active	Active
IOS IPS SDEE Server			
tti-petitioner	16	Active	Active
TTI Petitioner			

2. Create a list of session modules that are required, in this example it would be everything other than WEB_EXEC.

```
Router#configuration terminal
Router(config)#ip http session-module-list
exclude_webexec
HTTP_IFS,HOME_PAGE,QDM,QDM_SA,IXI,
IDCONF,XSM,VDM,XML_Api,
ITS,ITS_LOCDIR,CME_SERVICE_URL,
CME_AUTH_SRV_LOGIN,IPS_SDEE,tti-petitioner
```

3. Selectively enable HTTP/HTTPS applications that will service incoming HTTP requests from remote clients.

```
Router(config)#ip http active-session-modules
exclude_webexec
Router(config)#ip http secure-active-session-modules
exclude_webexec
Router(config)#exit
```

4. Verify the list of all session modules, and ensure WEB_EXEC is not active.

```
Router#show ip http server session-module
HTTP server application session modules:
  Session module Name  Handle Status    Secure-status
Description
HTTP_IFS                1      Active    Active
HTTP based IOS File Server
HOME_PAGE                2      Active    Active
```

IOS Homepage Server			
QDM	3	Active	Active
QOS Device Manager Server			
QDM_SA	4	Active	Active
QOS Device Manager Signed Applet Server			
WEB_EXEC	5	Inactive	Inactive
HTTP based IOS EXEC Server			
IXI	6	Active	Active
IOS XML Infra Application Server			
IDCONF	7	Active	Active
IDCONF HTTP(S) Server			
XSM	8	Active	Active
XML Session Manager			
VDM	9	Active	Active
VPN Device Manager Server			
XML_Api	10	Active	Active
XML Api			
ITS	11	Active	Active
IOS Telephony Service			
ITS_LOCDIR	12	Active	Active
ITS Local Directory Search			
CME_SERVICE_URL	13	Active	Active
CME Service URL			
CME_AUTH_SRV_LOGIN	14	Active	Active
CME Authentication Server			
IPS_SDEE	15	Active	Active
IOS IPS SDEE Server			
tti-petitioner	16	Active	Active
TTI Petitioner			

For further information on selective enabling of applications using an HTTP or secure HTTP server, consult the Cisco IOS network management configuration guide, release 12.4T at: http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_http_app_enable.html

Avoid the use of Web-based SHOW commands

Successful exploitation of this vulnerability requires an unsuspecting user to request dynamic content from the device via the "show" commands which are available. Avoiding the use of those commands via the web interface until an upgrade to fixed software is possible may be perfectly legitimate for some installations.

☐ **Obtaining Fixed Software**

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. 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.

[Top of the section](#) [Close Section](#)

☐ **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>.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ 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.

[Top of the section](#) [Close Section](#)

☐ Exploitation and Public Announcements

This vulnerability was disclosed in a public posting to the Bugtraq mailing list, and at the following URL: http://www.infohacking.com/INFOHACKING_RESEARCH/Our_Advisories/cisco/index.html .

We would like to thank iDefense for finding and initially reporting this vulnerability to us.

We would also like to thank Mr. Adrian Pastor from ProCheckup Ltd for sharing information with us about another possible vector into this vulnerability. His research paper is available at http://www.procheckup.com/vulnerability_manager/vulnerabilities/paper-04 .

The Cisco PSIRT is not aware of any malicious use of the vulnerability described in this advisory.

[Top of the section](#) [Close Section](#)

☐ 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.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.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.

[Top of the section](#) [Close Section](#)

☐ **Revision History**

Revision 1.3	22-October-2009	Updated the Exploitation and Public Announcements to include additional researcher information.
Revision 1.2	19-June-2009	Revised the <i>Disable the HTTP WEB_EXEC Service</i> section.
Revision 1.1	14-January-2006	Added additional advisory credits.
Revision 1.0	1-December-2005	Initial public release.

[Top of the section](#) [Close Section](#)

☐ 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/>.

[Top of the section](#) [Close Section](#)

Help us help you.



Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor



This document solved my problem.

- Yes
- No
- Just browsing



Suggestions for improvement:

(256 character limit)

[Home](#)[How to Buy](#)[Login](#)[Profile](#)[Feedback](#)[Site Map](#)[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

[Trademarks of Cisco Systems, Inc.](#)