

Cisco Security Response: Cisco IOS Cross-Site Scripting Vulnerabilities

<http://www.cisco.com/warp/public/707/cisco-sr-20090114-http.shtml>

Revision 3.1

Last Updated 2009 June 19 2100 UTC (GMT)

For Public Release 2009 January 14 1600 UTC (GMT)

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

Contents

[Cisco Response](#)

[Additional Information](#)

[Status of this Notice: INTERIM](#)

[Revision History](#)

[Cisco Security Procedures](#)

Cisco Response

Three separate Cisco IOS[®] Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers. ProCheckup has posted a Security Advisory titled "XSS on Cisco IOS HTTP Server" posted at http://www.procheckup.com/vulnerability_manager/vulnerabilities/pr08-19.

Cisco would like to thank Adrian Pastor and Richard J. Brain of ProCheckUp and Nobuhiro Tsuji of NTT Data Security Corporation with co-operation of JPCert.

This Cisco Security Response is posted at the following link: <http://www.cisco.com/warp/public/707/cisco-sr-20090114-http.shtml>.

Additional Information

This response covers three separate cross-site scripting vulnerabilities within the Cisco IOS Hypertext Transfer Protocol (HTTP) server (including HTTP secure server - here after referred to as purely HTTP Server) and a cross-site request forgery (CSRF) vulnerability and applies to all Cisco products that run Cisco IOS Software versions 11.0 through 12.4 with the HTTP server enabled for HTTP based IOS EXEC Server. A system that 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 | include status** and the **show ip http server secure status | include status** commands at the prompt and look for output similar to:

```
Router#show ip http server status | include status  
HTTP server status: Enabled  
HTTP secure server status: Enabled
```

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

```
Router#show ip http server status | include status  
HTTP server status: Disabled  
HTTP secure server status: Disabled
```

These vulnerabilities are documented in the following Cisco bug IDs:

- Cisco bug ID [CSCsi13344 - XSS in IOS HTTP Server](#) ([registered](#) customers only)
Special Characters are not escaped in URL strings sent to the HTTP server.
- Cisco bug ID [CSCsr72301 - XSS in IOS HTTP Server \(ping parameter\)](#) ([registered](#) customers only)
Special Characters are not escaped in URL strings sent to the HTTP server, via the **ping** parameter. The ping parameter is used both by external applications such as Router and Security Device Manager (SDM) as well as a direct HTTP session to Cisco IOS http server. This vulnerability affects 12.1E based trains and all Cisco IOS releases after 12.2(13)T.
- Cisco bug ID [CSCsv05154 - Cisco IOS HTTP Server vulnerable to CSRF attacks](#) ([registered](#) customers only)

The Cisco IOS HTTP server enabled with HTTP based IOS EXEC Server is vulnerable to Cross-Site Request Forgery attacks - which may allow malicious users to execute commands on the device through the web interface under the privileges of an already logged-in user.

- Cisco bug ID [CSCsx49573 - XSS in Cisco IOS HTTP Server](#) ([registered](#) customers only)

This is an extension to Cisco Bug ID CSCsi13344, which did not provide a complete fix against XSS attacks to the Cisco IOS HTTP Server enabled for HTTP based IOS EXEC Server.

These vulnerabilities are independent of each other. For a full solution, download a Cisco IOS version that contains the fixes for all Cisco bug IDs. These vulnerabilities have been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-3821.

Workaround:

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

Access Control

If the HTTP server is required, it is a recommended best practice to control which hosts may access the HTTP server to only trusted sources. To control which hosts can access the HTTP server, you can apply an access list to the HTTP server. To apply an access list to the HTTP server, use the following command in global configuration mode:

```
ip http access-class {access-list-number | access-list-name}
```

The following example shows an access list that allows only trusted hosts to access the Cisco IOS HTTP server:

```
ip access-list standard 20
  permit 192.168.1.0 0.0.0.255
  remark "Above is a trusted subnet"
  remark "Add further trusted subnets or hosts below"
```

```
! (Note: all other access implicitly denied)
! (Apply the access-list to the http server)
```

```
ip http access-class 20
```

For additional information on configuring the Cisco IOS HTTP server, consult [Using the Cisco Web Browser User Interface](#).

For additional information on cross-site scripting attacks and the methods used to exploit these vulnerabilities, please refer to the Cisco Applied Mitigation Bulletin "Understanding Cross-Site Scripting (XSS) Threat Vectors", which is available at the following link: <http://www.cisco.com/warp/public/707/cisco-amb-20060922-understanding-xss.shtml>.

Further Problem Description:

This vulnerability is about escaping characters in the URL that are sent to the HTTP server. This

vulnerability is different from the vulnerability reported in Cisco bug ID [CSCsc64976](#) ([registered](#) customers only) . The fix for this vulnerability is to escape special characters in the URL string echoed in the response generated by the web exec application.

Software Version and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

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. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Cisco is currently patching these Cisco bug IDs into Cisco IOS software. To check on the latest versions with fixed releases please consult the Cisco Bug Toolkit <http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs> or click on the Cisco Bug IDs within the Cisco Response section of this response.

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.

Revision History

Revision 3.1	19-June-2009	Revised the <i>Disable the HTTP WEB_EXEC Service</i> section.

Revision 3.0	2009-February-06	Updated Additional Information and Software Versions and Fixes
Revision 2.0	2009-January-23	Updated software table
Revision 1.0	2009-January-14	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>.

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.](#)