Updated: May 31, 2014 **Document ID:** 1454785010982871

Cisco Security Advisory

Cisco IOS Software Command Authorization Bypass

Critical

Advisory ID:
cisco-sa-20120328-pai

First Published:
2012 March 28 16:00 GMT

Version 1.0: Final

Workarounds: See below

Cisco Bug IDs:
CSCtr91106

CVE-2012-0384

CVSS Score:
Base 9.0, Temporal 7.4 **Click Icon to Copy Verbose Score**
AV:N/AC:L/Au:S/C:C/I:C/A:C/E:F/RL:OF/RC:C

Download CVRF Download OVAL Email

Summary

A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS Software are not vulnerable.

Cisco has released software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai
Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities

in the March 2012 bundled publication.

Individual publication links are in "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

Affected Products

Vulnerable Products

Any device running Cisco IOS Software release after 12.2 that has an HTTP or HTTPS server configured is affected by this vulnerability if AAA authorization is used.
To determine if an HTTP or HTTP server is configured with an HTTP or HTTPS server, issue the show ip http server status | include status command. The following example illustrates a Cisco IOS device with an HTTPS server enabled and the HTTP server disabled.

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

To determine if AAA authorization is used, an administrator can log in to the device and issue the **show run | include aaa authorization** command in privileged EXEC mode. If there is an entry that shows **aaa authorization commands**, as shown in the following example, then AAA authorization is configured.

```
Router# show run | include aaa authorization commands
 aaa authorization commands 0 default local group tacacs+
 aaa authorization commands 1 default group tacacs+
 aaa authorization commands 15 default local
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the **show version** command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 15.0(1)M1 with an installed image name of C3900-UNIVERSALK9-M:

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1,
RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
!--- output truncated
```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS and NX-OS Software Reference Guide" at http://www.cisco.com/web/about/security/intelligence/ios-ref.html.

Products Confirmed Not Vulnerable

If you are not running Cisco IOS or IOS XE Software, you are not affected by this vulnerability. Devices that are not using AAA authorization or that do not have an HTTP or HTTPS server configured are not affected by this vulnerability.

Cisco IOS XR is not affected by this vulnerability.

No other Cisco products are currently known to be affected by this vulnerability.

Details

Cisco IOS Software allows remote applications to administer and monitor devices running Cisco IOS Software over an HTTP or HTTPS connection.

A vulnerability exists that may allow the Cisco IOS command authorization to be bypassed, allowing a remote, authenticated HTTP or HTTPS session to execute any Cisco IOS command that is configured for their authorization level. This vulnerability does not allow unauthenticated access; a valid username and password are required to successfully exploit this vulnerability. Additionally, the vulnerability does not allow a user to execute commands that are not configured for their privilege level.

The HTTP server is enabled by default for cluster configurations and on the following Cisco switches: Catalyst 3700 series, Catalyst 3750 series, Catalyst 3550 series, Catalyst 3560 series, and Catalyst 2950 series.

More information on AAA authorization can be found at: http://www.cisco.com/en/US/docs/ios/12_2t/secure/command/reference/sftauth.html.

Releases of Cisco IOS Software after release 12.2 are potentially vulnerable. Please refer to the release table below for more information.

This vulnerability is documented as Cisco Bug ID CSCtr91106 (registered customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2012-0384.

Workarounds

If the HTTP and HTTPS servers are not required, they may be disabled with the commands **no ip http server** and **no ip http secure-server**.

However, if web services are required, 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 device and retrieve the current state of the device 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 the 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

If the HTTP server and WEB_EXEC service are required, it is a recommended best practice to limit which hosts may access the HTTP server to allow only trusted sources. An access list can be applied to the HTTP server to limit which hosts are permitted access. 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.

Fixed Software

When considering software upgrades, customers are advised to consult the Cisco Security Advisories and Responses archive at http://www.cisco.com/go/psirt and review subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Cisco IOS Software

Each row of the following Cisco IOS Software table corresponds to a Cisco IOS Software train. If a particular train is vulnerable, the earliest releases that contain the fix are listed in the First Fixed Release column. The First Fixed Release for All Advisories in the March 2012 Bundled Publication column lists the earliest possible releases that correct all the published vulnerabilities in the Cisco IOS Software Security Advisory bundled publication. Cisco recommends upgrading to the latest available release, where possible.

The Cisco IOS Software Checker allows customers to search for Cisco Security Advisories that address specific Cisco IOS Software releases. This tool is available on the Cisco Security (SIO) portal at https://sec.cloudapps.cisco.com/security/center/selectIOSVersion.x

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication**
There are no affected 12.0 based releases		
Affected 12.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication**
12.2	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2B	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2BC	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2BW	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2BX	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2BY	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2BZ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2CX	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2CY	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2CZ	Not vulnerable	Vulnerable; First fixed in Release 12.0S
12.2DA	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2DD	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2DX	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2EU	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2EW	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. Releases up to and including 12.2(20)EWA4	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.

	are not vulnerable.	
12.2EWA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. Releases up to and including 12.2(20)EWA4 are not vulnerable.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2EX	Vulnerable; First fixed in Release 15.0SE Releases up to and including 12.2(25)EX1 are not vulnerable.	Vulnerable; First fixed in Release 15.0SE
12.2EY	12.2(52)EY4 12.2(58)EY2	12.2(52)EY4
12.2EZ	Vulnerable; First fixed in Release 15.0SE	Vulnerable; First fixed in Release 15.0SE
12.2FX	Vulnerable; First fixed in Release 12.2SE	Vulnerable; First fixed in Release 15.0SE
12.2FY	Vulnerable; First fixed in Release 15.0SE	Vulnerable; First fixed in Release 15.0SE
12.2FZ	Vulnerable; First fixed in Release 12.2SE	Vulnerable; First fixed in Release 15.0SE
12.2IRA	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2IRB	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2IRC	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2IRD	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2IRE	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2IRF	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2IRG	Vulnerable; contact your support	Vulnerable; contact your support organization per the instructions in Obtaining

	organization per the instructions in Obtaining Fixed Software section of this advisory.	Fixed Software section of this advisory.
12.2IRH	12.2(33)IRH1	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXB	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXC	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXD	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXE	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXF	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2JA	Not vulnerable	Not vulnerable
12.2JK	Not vulnerable	Not vulnerable
12.2MB	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2MC	Not vulnerable	Vulnerable; First fixed in Release 15.0M

12.2MRA	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2MRB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2S	Not vulnerable	Releases prior to 12.2(30)S are vulnerable; Releases 12.2(30)S and later are not vulnerable. First fixed in Release 12.0S
12.2SB	12.2(33)SB12	12.2(33)SB12
12.2SBC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SCA	Vulnerable; First fixed in Release 12.2SCE	Vulnerable; First fixed in Release 12.2SCE
12.2SCB	Vulnerable; First fixed in Release 12.2SCE	Vulnerable; First fixed in Release 12.2SCE
12.2SCC	Vulnerable; First fixed in Release 12.2SCE	Vulnerable; First fixed in Release 12.2SCE
12.2SCD	Vulnerable; First fixed in Release 12.2SCE	Vulnerable; First fixed in Release 12.2SCE
12.2SCE	12.2(33)SCE5	12.2(33)SCE6
12.2SCF	12.2(33)SCF2	12.2(33)SCF2
12.2SE	12.2(55)SE5	12.2(55)SE5 *
12.2SEA	Vulnerable; First fixed in Release 12.2SE	Vulnerable; First fixed in Release 15.0SE
12.2SEB	Vulnerable; First fixed in Release 12.2SE	Vulnerable; First fixed in Release 15.0SE
12.2SEC	Vulnerable; First fixed in Release 12.2SE	Vulnerable; First fixed in Release 15.0SE
12.2SED	Vulnerable; First fixed in Release 12.2SE	Vulnerable; First fixed in Release 15.0SE
12.2SEE	Vulnerable; First fixed in Release 12.2SE	Vulnerable; First fixed in Release 15.0SE
12.2SEF	Vulnerable; First fixed in Release 12.2SE	Vulnerable; First fixed in Release 15.0SE

12.2SEG	Vulnerable; First fixed in Release 15.0SE	Vulnerable; First fixed in Release 15.0SE
12.2SG	12.2(53)SG7; Available on 07-MAY-12	12.2(53)SG7; Available on 07-MAY-12
12.2SGA	Vulnerable; First fixed in Release 12.2SG	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SL	Not vulnerable	Not vulnerable
12.2SM	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SO	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SQ	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SRA	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2SRB	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2SRC	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2SRD	12.2(33)SRD8	Vulnerable; First fixed in Release 12.2SRE
12.2SRE	12.2(33)SRE6	12.2(33)SRE6
12.2STE	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SU	Not vulnerable	Vulnerable; First fixed in Release 15.0M

12.2SV	Not vulnerable	Releases up to and including 12.2(18)SV2 are not vulnerable.
12.2SVA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SVC	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SVD	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SVE	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SW	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.2SX	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXB	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXD	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXE	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXF	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXH	Vulnerable; contact your support organization per	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of

	the instructions in Obtaining Fixed Software section of this advisory.	this advisory.
12.2SXI	12.2(33)SXI9	12.2(33)SXI9
12.2SXJ	12.2(33)SXJ2	12.2(33)SXJ2
12.2SY	12.2(50)SY2; Available on 11-JUN-12 Releases up to and including 12.2(14)SY5 are not vulnerable.	12.2(50)SY2; Available on 11-JUN-12
12.2SZ	Not vulnerable	Vulnerable; First fixed in Release 12.0S
12.2T	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2TPC	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2XA	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XB	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XC	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XD	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XE	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XF	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XG	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XH	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XI	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XJ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XK	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XL	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XM	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XNA	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability

12.2XNB	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNC	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XND	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNE	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNF	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XO	Vulnerable; First fixed in Release 12.2SG	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2XQ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XR	Not vulnerable	Releases prior to 12.2(15)XR are vulnerable; Releases 12.2(15)XR and later are not vulnerable. First fixed in Release 15.0M
12.2XS	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XT	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XU	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XV	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XW	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2YA	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2YC	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YD	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.

12.2YE	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YK	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YO	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YP	Not vulnerable	Vulnerable; First fixed in Release 15.0M Releases up to and including 12.2(8)YP are not vulnerable.
12.2YT	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YW	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YX	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YY	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YZ	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZB	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZC	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.

12.2ZD	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZE	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2ZH	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.2ZJ	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZP	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZU	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZX	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2ZY	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZYA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
Affected 12.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication**
12.3	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3B	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3BC	Vulnerable; First fixed in Release 12.2SCE	Vulnerable; First fixed in Release 12.2SCE
12.3BW	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3JA	Vulnerable; First fixed in Release 12.4JA	Vulnerable; First fixed in Release 12.4JA

12.3JEA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3JEB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3JEC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3JED	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3JK	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3JL	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3JX	Not vulnerable	Not vulnerable
12.3T	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3TPC	Vulnerable; contact your support organization per	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of

	the instructions in Obtaining Fixed Software section of this advisory.	this advisory.
12.3VA	Not vulnerable	Not vulnerable
12.3XA	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3XB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3XC	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3XD	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3XE	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3XF	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3XG	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3XI	Vulnerable; First fixed in Release 12.2SB	Vulnerable; First fixed in Release 12.2SRE
12.3XJ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3XK	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3XL	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3XQ	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M

12.3XR	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3XU	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.3XW	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3XX	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3XY	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3XZ	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 15.0M
12.3YD	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YF	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YG	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YI	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YJ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YK	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YM	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YQ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YS	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YT	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YU	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YX	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M

12.3YZ	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3ZA	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M

Affected 12.4-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication
12.4	12.4(25g); Available on 19-SEP-12	Vulnerable; First fixed in Release 15.0M
12.4GC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JA	12.4(23c)JA4 12.4(25d)JA2; Available on 01-AUG-12 12.4(25e)JA	12.4(23c)JA412.4(25e)JA
12.4JAX	Vulnerable; First fixed in Release 12.4JA	Vulnerable; First fixed in Release 12.4JA
12.4JDA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JDC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.

12.4JDD	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JDE	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JHA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JHB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JHC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JK	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.

12.4JL	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JX	Vulnerable; First fixed in Release 12.4JA	Vulnerable; First fixed in Release 12.4JA
12.4JY	Vulnerable; First fixed in Release 12.4JA	Vulnerable; First fixed in Release 12.4JA
12.4JZ	Vulnerable; First fixed in Release 12.4JA	Vulnerable; First fixed in Release 12.4JA
12.4MD	12.4(22)MD3; Available on 30-MAR-12	12.4(22)MD3; Available on 30-MAR-12
12.4MDA	12.4(24)MDA11	12.4(24)MDA11
12.4MDB	12.4(24)MDB5a	12.4(24)MDB5a
12.4MDC	Not vulnerable	Not vulnerable
12.4MR	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4MRA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4MRB	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4SW	12.4(15)SW8a	Vulnerable; First fixed in Release 15.0M
12.4T	12.4(15)T17 12.4(24)T7	12.4(15)T17 12.4(24)T7
12.4XA	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M

12.4XB	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.4XC	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XD	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XE	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XF	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XG	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XJ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XK	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XL	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XM	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XN	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XP	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.

12.4XQ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XR	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.4XT	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XV	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XW	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XY	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XZ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4YA	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4YB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4YD	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4YE	12.4(24)YE3d	12.4(24)YE3d
12.4YG	12.4(24)YG4	12.4(24)YG4

Affected 15.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication

15.0M	15.0(1)M8	15.0(1)M8
15.0MR	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.0MRA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.0S	15.0(1)S5 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.0(1)S5 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SA	Not vulnerable	Not vulnerable
15.0SE	15.0(1)SE1 15.0(2)SE; Available on 06-AUG-12	15.0(1)SE1
15.0SG	15.0(2)SG2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.0(2)SG2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SY	15.0(1)SY1	15.0(1)SY1
15.0XA	Vulnerable; First fixed in Release 15.1T	Vulnerable; First fixed in Release 15.1T
15.0XO	Vulnerable; First fixed in Release 15.0SG Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Vulnerable; First fixed in Release 15.0SG Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
Affected 15.1-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.1EY	15.1(2)EY1a	15.1(2)EY2
15.1GC	15.1(2)GC2	15.1(2)GC2

15.1M	15.1(4)M2	15.1(4)M4; Available on 30-MAR-12
15.1MR	15.1(1)MR3	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1S	15.1(3)S2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(3)S2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SG	Not vulnerable	Not vulnerable
15.1SNG	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SNH	Not vulnerable	Not vulnerable
15.1T	15.1(1)T4 15.1(2)T5; Available on 27-APR-12 15.1(3)T3	15.1(3)T3
15.1XB	Vulnerable; First fixed in Release 15.1T	Vulnerable; First fixed in Release 15.1T
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.2GC	15.2(1)GC1	15.2(1)GC2
15.2S	15.2(1)S1 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.2(1)S1 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.2T	15.2(1)T1 15.2(2)T 15.2(2)T1	15.2(1)T215.2(2)T115.2(3)T; Available on 30-MAR-12

* Cisco Catalyst 3550 Series Switches support the Internet Key Exchange (IKE) feature and are vulnerable to Cisco bug ID CSCts38429 when the devices are running Layer 3 images; however, this product reached the End of Software Maintenance milestone. Cisco 3550 Series SMI Switches that are running Layer 2 images do not support IKE and are not vulnerable. No other Cisco devices that run 12.2SE-based software are vulnerable.

Cisco IOS XE Software

Cisco IOS XE Software is affected by the vulnerability that is disclosed in this document.

Cisco IOS XE Software Release	First Fixed Release	First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication
2.1.x	Vulnerable; migrate to 3.1.2S or later.	Vulnerable; migrate to 3.4.2S or later.
2.2.x	Vulnerable; migrate to 3.1.2S or later.	Vulnerable; migrate to 3.4.2S or later.
2.3.x	Vulnerable; migrate to 3.1.2S or later.	Vulnerable; migrate to 3.4.2S or later.
2.4.x	Vulnerable; migrate to 3.1.2S or later.	Vulnerable; migrate to 3.4.2S or later.
2.5.x	Vulnerable; migrate to 3.1.2S or later.	Vulnerable; migrate to 3.4.2S or later.
2.6.x	Vulnerable; migrate to 3.1.2S or later.	Vulnerable; migrate to 3.4.2S or later.
3.1.xS	3.1.2S	Vulnerable; migrate to 3.4.2S or later.
3.1.xSG	Vulnerable; migrate to 3.2.2SG or later.	Vulnerable; migrate to 3.2.2SG or later.
3.2.xS	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
3.2.xSG	3.2.2SG	3.2.2SG
3.3.xS	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
3.2.xSG	Not vulnerable	Not vulnerable
3.4.xS	3.4.2S	3.4.2S
3.5.xS	3.5.1S	3.5.1S
3.6.xS	Not vulnerable	Not vulnerable

For a mapping of Cisco IOS XE Software releases to Cisco IOS Software releases, refer to Cisco IOS XE 2 Release Notes, Cisco IOS XE 3S Release Notes, and Cisco IOS XE 3SG Release Notes.

Cisco IOS XR Software

Cisco IOS XR Software is not affected by any of the vulnerabilities disclosed in the March 2012 Cisco IOS Software Security Advisory Bundled Publication.

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

This vulnerability was reported to Cisco TAC by customers observing the vulnerability during the normal operation of their devices.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

Revision History

Revision 1.0	2012-March-28	Initial public release

Legal Disclaimer

▶ Cisco Security Vulnerability Policy

▶ Subscribe to Cisco Security Notifications

▶ Related to This Advisory

Quick Links

About Cisco

Contact Us

Careers

Connect with a partner

Resources and Legal

Feedback

Help

Terms & Conditions

Privacy

Cookies / Do not sell or share my personal data

Accessibility

Trademarks

Supply Chain Transparency

Newsroom

Sitemap