Cisco Security Advisory

Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability

High

Advisory ID:	cisco-sa-20120926-sip
Last Updated:	2012 October 3 17:48 GMT
Published:	2012 September 26 16:00 GMT
Version1.1:	Final
CVSS Score:	Base - 7.8
Workarounds:	See below
Cisco Bug IDs:	CSCtj33003 CSCtw66721 CSCtw84664

CVE-2012-3949
CWE-399

Download CVRF

Download Oval

Download PDF

Email

Summary

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

Cisco has released software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

Note: The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each Cisco IOS Software Security 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 Cisco IOS Software vulnerabilities in the September 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_sep12.html

Cisco Unified Communications Manager is affected by the vulnerability described in this advisory. A separate Cisco Security Advisory has been published to disclose the vulnerability that affects the Cisco Unified Communications Manager at the following location:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-cucm

Affected Products

Vulnerable Products

Cisco devices that are running affected Cisco IOS Software or Cisco IOS XE Software versions are vulnerable when they are configured to process SIP messages and when pass-through of Session Description Protocol (SDP) is enabled.

Recent versions of Cisco IOS Software do not process SIP messages by default. Creating a dial peer by issuing the **dial-peer voice** configuration command will start the SIP processes, causing the Cisco IOS device to process SIP messages. In addition, several features within Cisco Unified Communications Manager Express, such as ePhones, will also automatically start the SIP process when they are configured, causing the device to start processing SIP messages. The following is an example of an affected configuration:

```
dial-peer voice Voice dial-peer tag voip
 ...
!
```

In addition to inspecting the Cisco IOS device configuration for a **dial-peer** command that causes the device to process SIP messages, administrators can also use the **show processes | include SIP** command to determine whether Cisco IOS Software is running the processes that handle SIP messages. In the following example, the presence of the processes **CCSIP_UDP_SOCKET** or **CCSIP_TCP_SOCKET** indicates that the Cisco IOS device will process SIP messages:

```
Router# show processes | include SIP
 149 Mwe 40F48254            4          1    400023108/24000  0 CCSIP_UDP_SOCKET
 150 Mwe 40F48034            4          1    400023388/24000  0 CCSIP_TCP_SOCKET
```

Note: Because there are several ways a device running Cisco IOS Software can start processing SIP messages, it is recommended that the **show processes | include SIP** command be used to determine whether the device is processing SIP messages instead of relying on the presence of specific configuration commands.

A device is only affected when SIP is enabled and when SDP pass-through is enabled at the global level or dial-peer level. At the global level, SDP pass-through is configured as follows:

```
voice service voip
 sip

  pass-thru content sdp
```

At the dial-peer level, SDP pass-through is configured as follows:

```
dial-peer voice peer ID voip

 voice-class sip pass-thru content sdp
```

Cisco Unified Border Element (Enterprise) images are also affected by this vulnerability.

Note: The Cisco Unified Border Element feature (CUBE), previously known as the Cisco Multiservice IP-to-IP Gateway, is a special Cisco IOS Software image that runs on Cisco multiservice gateway platforms. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking.

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.

Cisco IOS XE Software is affected by this vulnerability.

Note: Cisco Unified Communications Manager is affected by the vulnerability described in this advisory. A separate Cisco Security Advisory has been published to disclose the vulnerability that affects the Cisco Unified Communications Manager at the following location:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-cucm

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Related Resources

ERP Cisco_ERP_sep12

BLG Cisco IOS Software Security Advisory Bundle Announced

IS Cisco IOS Software and Cisco Unified Communications Manager Session Initiation Protocol Denial of Service Vulnerability

AMB Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager and Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability

Subscribe to Cisco Security Notifications

Subscribe

Products Confirmed Not Vulnerable

The SIP Application Layer Gateway (ALG), which is used by the Cisco IOS Network Address Translation (NAT) and firewall features of Cisco IOS Software, is not affected by this vulnerability.

Cisco Unified Border Element (SP Edition) is not affected by this vulnerability.

Cisco IOS XR Software is not affected by this vulnerability.

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

Details

Session Initiation Protocol (SIP) is a popular signaling protocol that is used to manage voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination. Voice and video are the most popular types of sessions that SIP handles, but the protocol has the flexibility to accommodate other applications that require call setup and termination. SIP call signaling can use UDP (port 5060), TCP (port 5060), or Transport Layer Security (TLS; TCP port 5061) as the underlying transport protocol.

A vulnerability exists in the SIP implementation in Cisco IOS Software and Cisco IOS XE Software that could allow a remote attacker to cause an affected device to reload. This vulnerability is triggered when an affected device processes a crafted SIP message that contains a valid Session Description Protocol (SDP) message. Only traffic destined to the device can trigger the vulnerability; transit SIP traffic is not an exploit vector. SDP pass-through must be enabled, either at the global level, or at the dial-peer level, for a device to be affected by this vulnerability.

Note: In cases where SIP is running over TCP transport, a TCP three-way handshake is necessary to exploit this vulnerability.

This vulnerability is documented in Cisco bug IDs CSCtj33003 (registered customers only) and CSCtw84664 (registered customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2012-3949.

Note: This vulnerability also affects Cisco Unified Communications Manager. The corresponding Cisco bug ID is CSCtw66721 (registered customers only). Refer to the separate Cisco Security Advisory for the Cisco Unified Communications Manager for additional details.

Workarounds

If the affected Cisco IOS device requires SIP and pass-through of SDP for VoIP services, then SIP and SDP pass-through cannot be disabled and no workarounds are available. Users are advised to apply mitigation techniques to help limit exposure to the vulnerabilities. Mitigation consists of allowing only legitimate devices to connect to affected devices. To increase effectiveness, the mitigation must be coupled with anti-spoofing measures on the network edge. This action is required because SIP can use UDP as the transport protocol.

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document "Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager and Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability", which is available at the following link:

http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=26765

Disabling SIP Listening Ports

For devices that do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device. Some versions of Cisco IOS Software allow administrators to disable SIP with the following commands:

```
sip-ua
 no transport udp
 no transport tcp
 no transport tcp tls
```

Warning: When applying this workaround to devices that are processing Media Gateway Control Protocol (MGCP) or H.323 calls, the devices will not stop SIP processing while active calls are being processed. Under these circumstances, this workaround should be implemented during a maintenance window when active calls can be briefly stopped.

The **show udp connections**, **show tcp brief all**, and **show processes | include SIP** commands can be used to confirm that the SIP UDP and TCP ports are closed after applying this workaround.

Depending on the Cisco IOS Software version in use, when SIP is disabled the output from the **show ip sockets** command may still show the SIP ports open, but sending traffic to them will cause the SIP process to emit the following message:

```
*Jul 27 15:22:41.251: sip_udp_sock_process_read: SIP UDP Listener is DISABLED
```

Disabling SDP Pass-Through

If SIP must remain enabled, but SDP pass-through is not required, then disabling SDP pass-through can be used as a workaround. SDP pass-through is disabled by default. SDP pass-through can be enabled at the global level, or at the dial peer level. Refer to the section "Affected Products" for details on how to disable SDP pass-through.

Control Plane Policing

For devices that must offer SIP services, it is possible to use Control Plane Policing (CoPP) to block SIP traffic to the device from untrusted sources. Cisco IOS Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to specific network configurations:

```
!-- The 192.168.1.0/24 network and the 172.16.1.1 host are trusted.
!-- Everything else is not trusted. The following access list is used
!-- to determine what traffic needs to be dropped by a control plane
!-- policy (the CoPP feature): if the access list matches (permit)
!-- then traffic will be dropped and if the access list does not
!-- match (deny) then traffic will be processed by the router.
access-list 100 deny udp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5061
access-list 100 deny udp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5061
access-list 100 permit udp any any eq 5060
access-list 100 permit tcp any any eq 5060
access-list 100 permit tcp any any eq 5061

!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!-- traffic in accordance with existing security policies and
!-- configurations for traffic that is authorized to be sent
!-- to infrastructure devices.
!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature.
class-map match-all drop-sip-class
  match access-group 100

!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.
policy-map control-plane-policy
 class drop-sip-class
  drop

!-- Apply the Policy-Map to the Control-Plane of the
!-- device.
control-plane
 service-policy input control-plane-policy
```

Note: Because SIP can use UDP as a transport protocol, it is possible to spoof the source address of an IP packet, which may bypass access control lists that permit communication to these ports from trusted IP addresses.

In the preceding CoPP example, the access control entries (ACEs) that match the potential exploit packets with the **permit** action result in these packets being discarded by the policy-map **drop** function, while packets that match the **deny** action (not shown) are not affected by the policy-map drop function. Additional information on the configuration and use of the CoPP feature can be found at http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html and http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html.

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 September 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 http://tools.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 September 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 September 2012 Cisco IOS Software Security Advisory Bundled Publication**
12.2	Not vulnerable	Not vulnerable
12.2B	Vulnerable; First fixed in Release 12.4 Releases up to and including 12.2(4)B8 are not vulnerable.	Vulnerable; First fixed in Release 12.4 Releases up to and including 12.2(4)B8 are not vulnerable.
12.2BC	Not vulnerable	Not vulnerable
12.2BW	Not vulnerable	Not vulnerable
12.2BX	Vulnerable; migrate to any release in 12.2SB Releases up to and including 12.2(15)BX are not vulnerable.	12.2(15)BX Releases up to and including 12.2(2)BX1 are not vulnerable.
12.2BY	Not vulnerable	Not vulnerable
12.2BZ	Not vulnerable	Not vulnerable
12.2CX	Not vulnerable	Not vulnerable
12.2CY	Not vulnerable	Not vulnerable
12.2CZ	Vulnerable; migrate to any release in 12.2S	Vulnerable; migrate to any release in 12.2S
12.2DA	Not vulnerable	Not vulnerable
12.2DD	Not vulnerable	Not vulnerable
12.2DX	Not vulnerable	Not vulnerable
12.2EU	Not vulnerable	Not vulnerable
12.2EW	Not vulnerable	Not vulnerable
12.2EWA	Not vulnerable	Not vulnerable
12.2EX	Not vulnerable	Vulnerable; First fixed in Release 15.0SE Releases up to and including 12.2(37)EX are not vulnerable.
12.2EY	Not vulnerable	Vulnerable; First fixed in Release 15.1EY Releases up to and including 12.2(46)EY are not vulnerable.
12.2EZ	Not vulnerable	Not vulnerable
12.2FX	Not vulnerable	Not vulnerable
12.2FY	Not vulnerable	Not vulnerable
12.2FZ	Not vulnerable	Not vulnerable
12.2IRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRB	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRD	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRE	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRF	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IRH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IRI	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXA	Not vulnerable	Not vulnerable
12.2IXB	Not vulnerable	Not vulnerable
12.2IXC	Not vulnerable	Not vulnerable
12.2IXD	Not vulnerable	Not vulnerable
12.2IXE	Not vulnerable	Not vulnerable
12.2IXF	Not vulnerable	Not vulnerable
12.2IXG	Not vulnerable	Not vulnerable
12.2IXH	Not vulnerable	Not vulnerable
12.2JA	Not vulnerable	Not vulnerable
12.2JK	Not vulnerable	Not vulnerable
12.2MB	Not vulnerable	Not vulnerable
12.2MC	Releases up to and including 12.2(15)MC1 are not vulnerable. Releases 12.2(15)MC2b and later are not vulnerable. First fixed in Release 12.4	Releases up to and including 12.2(15)MC1 are not vulnerable. Releases 12.2(15)MC2b and later are not vulnerable. First fixed in Release 12.4
12.2MRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2MRB	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2S	Not vulnerable	Not vulnerable
12.2SB	Not vulnerable	12.2(33)SB13
12.2SBC	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2SCA	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCB	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCC	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCD	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCE	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCF	Not vulnerable	12.2(33)SCF4
12.2SCG	Not vulnerable	Not vulnerable
12.2SE	Not vulnerable	12.2(46)SE1 12.2(55)SE6
12.2SEA	Not vulnerable	Not vulnerable
12.2SEB	Not vulnerable	Not vulnerable
12.2SEC	Not vulnerable	Not vulnerable
12.2SED	Not vulnerable	Not vulnerable
12.2SEE	Not vulnerable	Not vulnerable
12.2SEF	Not vulnerable	Not vulnerable
12.2SEG	Not vulnerable	Not vulnerable
12.2SG	Not vulnerable	12.2(53)SG8 Vulnerable; releases up to and including 12.2(46)SG1 are not vulnerable.
12.2SGA	Not vulnerable	Not vulnerable
12.2SM	Not vulnerable	Not vulnerable
12.2SO	Not vulnerable	Not vulnerable
12.2SQ	Not vulnerable	Releases up to and including 12.2(44)SQ2 are not vulnerable.
12.2SRA	Not vulnerable	Not vulnerable
12.2SRB	Not vulnerable	Not vulnerable
12.2SRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRD	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRE	Not vulnerable	12.2(33)SRE7
12.2STE	Not vulnerable	Not vulnerable
12.2SU	Not vulnerable	Not vulnerable
12.2SV	Not vulnerable	Not vulnerable
12.2SVA	Not vulnerable	Not vulnerable
12.2SVC	Not vulnerable	Not vulnerable
12.2SVD	Not vulnerable	Not vulnerable
12.2SVE	Not vulnerable	Not vulnerable
12.2SW	Not vulnerable	Not vulnerable

12.2SX	Not vulnerable	Not vulnerable
12.2SXA	Not vulnerable	Not vulnerable
12.2SXB	Not vulnerable	Not vulnerable
12.2SXD	Not vulnerable	Not vulnerable
12.2SXE	Not vulnerable	Not vulnerable
12.2SXF	Not vulnerable	Not vulnerable
12.2SXH	Not vulnerable	Vulnerable; releases up to and including 12.2(33)SXH7 are not vulnerable
12.2SXI	Not vulnerable	12.2(33)SXI10
12.2SXJ	Not vulnerable	12.2(33)SXJ4
12.2SY	Not vulnerable	12.2(50)SY3
12.2SZ	Not vulnerable	Not vulnerable
12.2T	Vulnerable; First fixed in Release 12.4 Releases up to and including 12.2(8)T10 are not vulnerable.	Vulnerable; First fixed in Release 12.4 Releases up to and including 12.2(8)T10 are not vulnerable.
12.2TPC	Not vulnerable	Not vulnerable
12.2WO	Not vulnerable	Vulnerable; First fixed in Release 15.0SG
12.2XA	Not vulnerable	Not vulnerable
12.2XB	Not vulnerable	Not vulnerable
12.2XC	Not vulnerable	Not vulnerable
12.2XD	Not vulnerable	Not vulnerable
12.2XE	Not vulnerable	Not vulnerable
12.2XF	Not vulnerable	Not vulnerable
12.2XG	Not vulnerable	Not vulnerable
12.2XH	Not vulnerable	Not vulnerable
12.2XI	Not vulnerable	Not vulnerable
12.2XJ	Not vulnerable	Not vulnerable
12.2XK	Not vulnerable	Not vulnerable
12.2XL	Not vulnerable	Not vulnerable
12.2XM	Not vulnerable	Not vulnerable
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	Not vulnerable	Vulnerable; First fixed in Release 12.2SG Releases up to and including 12.2(40)XO are not vulnerable.
12.2XQ	Not vulnerable	Not vulnerable
12.2XR	Not vulnerable	Not vulnerable
12.2XS	Not vulnerable	Not vulnerable
12.2XT	Not vulnerable	Not vulnerable
12.2XU	Not vulnerable	Not vulnerable
12.2XV	Not vulnerable	Not vulnerable
12.2XW	Not vulnerable	Not vulnerable
12.2YA	Not vulnerable	Not vulnerable
12.2YC	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.
12.2YD	Not vulnerable	Not vulnerable
12.2YE	Not vulnerable	Not vulnerable
12.2YK	Not vulnerable	Not vulnerable
12.2YO	Not vulnerable	Not vulnerable
12.2YP	Not vulnerable	Not vulnerable
12.2YT	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.
12.2YW	Not vulnerable	Not vulnerable
12.2YX	Not vulnerable	Not vulnerable
12.2YY	Not vulnerable	Not vulnerable
12.2YZ	Not vulnerable	Not vulnerable
12.2ZA	Not vulnerable	Not vulnerable
12.2ZB	Not vulnerable	Not vulnerable
12.2ZC	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.
12.2ZD	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.
12.2ZE	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 12.4
12.2ZH	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 12.4
12.2ZJ	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.
12.2ZP	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.
12.2ZU	Not vulnerable	Not vulnerable
12.2ZX	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2ZY	Not vulnerable	Not vulnerable
12.2ZYA	Not vulnerable	Not vulnerable
Affected 12.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication**
12.3	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 12.4
12.3B	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 12.4
12.3BC	Not vulnerable	Not vulnerable
12.3BW	Not vulnerable	Not vulnerable
12.3JA	Not vulnerable	Not vulnerable
12.3JEA	Not vulnerable	Not vulnerable
12.3JEB	Not vulnerable	Not vulnerable
12.3JEC	Not vulnerable	Not vulnerable
12.3JED	Not vulnerable	Not vulnerable
12.3JEE	Not vulnerable	Not vulnerable
12.3JK	Releases up to and including 12.3(2)JK3 are not vulnerable. Releases 12.3(8)JK1 and later are not vulnerable. First fixed in Release 12.4	Releases up to and including 12.3(2)JK3 are not vulnerable. Releases 12.3(8)JK1 and later are not vulnerable. First fixed in Release 12.4
12.3JL	Not vulnerable	Not vulnerable
12.3JX	Not vulnerable	Not vulnerable
12.3T	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 12.4
12.3TPC	Releases up to and including 12.3(4)TPC11a are not vulnerable.	Releases up to and including 12.3(4)TPC11a are not vulnerable.
12.3VA	Not vulnerable	Not vulnerable
12.3XA	Releases prior to 12.3(2)XA7 are vulnerable; Releases 12.3(2)XA7 and later are not vulnerable. First fixed in Release 12.4	Releases prior to 12.3(2)XA7 are vulnerable; Releases 12.3(2)XA7 and later are not vulnerable. First fixed in Release 12.4
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 12.4
12.3XD	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 12.4
12.3XE	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 12.4
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 12.4
12.3XI	Vulnerable; migrate to any release in 12.2SB	12.3(7)XI1b

12.3XJ	Vulnerable; migrate to any release in 12.4XN	Vulnerable; First fixed in Release 12.4T
12.3XK	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 12.4
12.3XL	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.3XQ	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 12.4
12.3XR	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 12.4
12.3XU	Vulnerable; First fixed in Release 12.4T Releases up to and including 12.3(8)XU1 are not vulnerable.	Vulnerable; First fixed in Release 12.4T Releases up to and including 12.3(8)XU1 are not vulnerable.
12.3XW	Vulnerable; migrate to any release in 12.4XN	Vulnerable; First fixed in Release 12.4T
12.3XX	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 12.4
12.3XY	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 12.4
12.3XZ	Vulnerable; First fixed in Release 12.4	Vulnerable; First fixed in Release 12.4
12.3YD	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.3YF	Vulnerable; migrate to any release in 12.4XN	Vulnerable; First fixed in Release 12.4T
12.3YG	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.3YI	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.3YJ	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.3YK	Releases prior to 12.3(11)YK3 are vulnerable; Releases 12.3(11)YK3 and later are not vulnerable. First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.3YM	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.3YQ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.3YS	Vulnerable; First fixed in Release 12.4T Releases up to and including 12.3(11)YS1 are not vulnerable.	Vulnerable; First fixed in Release 12.4T
12.3YT	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.3YU	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.3YX	Vulnerable; migrate to any release in 12.4XN	Vulnerable; First fixed in Release 12.4T
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 12.4T
Affected 12.4-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication**
12.4	12.4(25g)	12.4(25g)
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	Not vulnerable	Not vulnerable
12.4JAL	Not vulnerable	Not vulnerable
12.4JAX	Not vulnerable	Not vulnerable
12.4JAY	Not vulnerable	Not vulnerable
12.4JDA	Not vulnerable	Not vulnerable
12.4JDC	Not vulnerable	Not vulnerable
12.4JDD	Not vulnerable	Not vulnerable
12.4JDE	Not vulnerable	Not vulnerable
12.4JHA	Not vulnerable	Not vulnerable
12.4JHB	Not vulnerable	Not vulnerable
12.4JHC	Not vulnerable	Not vulnerable
12.4JK	Not vulnerable	Not vulnerable
12.4JL	Not vulnerable	Not vulnerable
12.4JX	Not vulnerable	Not vulnerable
12.4JY	Not vulnerable	Not vulnerable
12.4JZ	Not vulnerable	Not vulnerable
12.4MD	Not vulnerable	12.4(24)MD7
12.4MDA	Not vulnerable	Releases up to and including 12.4(22)MDA6 are not vulnerable
12.4MDB	Not vulnerable	12.4(24)MDB10
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 12.4T
12.4SW	Not vulnerable	Not vulnerable
12.4T	12.4(15)T17 12.4(24)T7	12.4(24)T8
12.4XA	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.4XB	Releases prior to 12.4(2)XB12 are vulnerable; Releases 12.4(2)XB12 and later are not 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 12.4T
12.4XD	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.4XE	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.4XF	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XG	Releases up to and including 12.4(9)XG1 are not vulnerable. Releases 12.4(9)XG3 and later are not vulnerable. First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.4XJ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.4XK	Not vulnerable	Vulnerable; First fixed in Release 12.4T
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	Releases up to and including 12.4(15)XM are not vulnerable. Releases 12.4(15)XM3 and later are not vulnerable. First fixed in Release 12.4T	Releases up to and including 12.4(15)XM are not vulnerable. Releases 12.4(15)XM3 and later are not vulnerable. First fixed in Release 12.4T
12.4XN	Not vulnerable	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	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XR	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XT	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
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 12.4T
12.4XY	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.4XZ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.4YA	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
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	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4YE	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4YG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
Affected 15.0-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.0EX	Not vulnerable	Not vulnerable
15.0EY	Not vulnerable	Not vulnerable
15.0M	15.0(1)M9	15.0(1)M9

15.0MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.0MRA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.0S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.0(1)S6 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SE	Not vulnerable	15.0(2)SE
15.0SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.0(2)SG5 15.0(2)SG6; Available on 11-OCT-12 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SY	Not vulnerable	15.0(1)SY2
15.0XA	Vulnerable; First fixed in Release 15.1M	Vulnerable; First fixed in Release 15.1M
15.0XO	Cisco IOS XE devices: Please see Cisco IOS-XE Software Availability	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 September 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.1EY	Not vulnerable	15.1(2)EY4
15.1GC	Vulnerable; First fixed in Release 15.1M	Vulnerable; First fixed in Release 15.1M
15.1M	15.1(4)M5	15.1(4)M5
15.1MR	Not vulnerable	15.1(3)MR; Available on 01-OCT-12
15.1S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(3)S Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(1)SG1 15.1(2)SG 12-NOV-12 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SNG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SNH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SNI	Not vulnerable	Vulnerable; migrate to any release in 15.2SNG
15.1SV	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.
15.1T	Vulnerable; First fixed in Release 15.1M	Vulnerable; First fixed in Release 15.1M
15.1XB	Vulnerable; First fixed in Release 15.1M	Vulnerable; First fixed in Release 15.1M
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.2GC	Releases prior to 15.2(3)GC are vulnerable; Releases 15.2(3)GC and later are not vulnerable. First fixed in Release 15.2T	Releases prior to 15.2(3)GC are vulnerable; Releases 15.2(3)GC and later are not vulnerable. First fixed in Release 15.2T
15.2JA	Not vulnerable	Not Vulnerable
15.2M	Not vulnerable	Not vulnerable
15.2S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.2(1)S2 15.2(2)S1 15.2(4)S Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.2SNG	Not vulnerable	Not vulnerable
15.2T	15.2(1)T3 15.2(2)T2 15.2(3)T	15.2(1)T3 15.2(2)T2 15.2(3)T2; Available on 12-OCT-12

Cisco IOS XE Software

Cisco IOS XE Software Release	First Fixed Release	First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication
2.1.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.2.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.3.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.4.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.5.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.6.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
3.1.xS	Not vulnerable	3.1.4S
3.1.xSG	Not vulnerable	Vulnerable; migrate to 3.2.5SG or later.
3.2.xS	Not vulnerable	Not vulnerable
3.2.xSG	Not vulnerable	3.2.5SG
3.2.xXO	Not vulnerable	Vulnerable; migrate to 3.3.1SG or later.
3.3.xS	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
3.3.x.SG	3.3.1SG	3.3.1SG
3.4.xS	Vulnerable; migrate to 3.6.0S or later.	Vulnerable; migrate to 3.6.0S or later.
3.5.xS	Vulnerable; migrate to 3.6.0S or later.	Vulnerable; migrate to 3.6.0S or later.
3.6.xS	Not vulnerable	Not vulnerable
3.7.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 the vulnerability that is disclosed in this document.

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 found during troubleshooting of TAC service requests.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

---

Revision History

Revision 1.1	2012-October-03	Clarify that Cisco Unified Border Element (SP Edition) is not affected.
Revision 1.0	2012-September-26	Initial public release.

Legal Disclaimer