

Cisco Security Advisory: SIP Packets Reload IOS Devices with support for SIP

Advisory ID: cisco-sa-20070131-sip

<http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml>

Revision 2.1

Last Updated 2007 February 10 0400 UTC (GMT)

For Public Release 2007 January 31 0900 UTC (GMT)

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

Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Impact](#)
- [Software Version and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of this Notice:FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

Summary

Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP.

There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

Workarounds exist to mitigate the effects of this problem on devices which do not require SIP.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml>.

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

☐ Affected Products

☐ Vulnerable Products

Any Cisco device which runs a vulnerable version of IOS and supports SIP processing could be vulnerable. This includes IOS versions 12.3(4)XH, 12.3(4)XQ, 12.3(7)XR, 12.3(7)XS, 12.3(8)JA, 12.3(8)T, 12.3(8)XU, 12.3(8)XW, 12.3(8)XX, 12.3(8)XY, 12.3(8)YA, 12.3(8)YG, 12.3(8)YH, 12.3(8)YI, 12.3(8)ZA, 12.4 Mainline and 12.4T onward. Routers configured as SIP Public Switched Telephone Network (PSTN) Gateways are vulnerable, as are routers configured as SIP Session Border Controllers (SBCs) and the CAT6000-CMM card.

To determine if your device has SIP enabled, enter the commands **show ip sockets** and **show tcp brief all**. Below is an example of a router running code without the fix, and without the workaround enabled. The router in this example is running the vulnerable image c7200-p-mz.124-3.bin:

```
Router#show ip sockets
Proto Remote      Port      Local      Port  In Out Stat TTY OutputIF
17 0.0.0.0          0  --any--  5060    0  0  211  0
17 0.0.0.0          0 192.168.100.2  67    0  0  2211  0
17 0.0.0.0          0 192.168.100.2  2517  0  0   11  0
```

The first line with UDP Port 5060 shows that UDP SIP is enabled.

```
Router#show tcp brief all
TCB      Local Address      Foreign Address      (state)
2051E680 *.5060              *.*                  LISTEN
```

The above lines with *.5060 show that TCP SIP is enabled.

☐ Products Confirmed Not Vulnerable

Devices that do not support SIP processing are not affected by this issue. This includes but is not limited to the 6500, 7600, 10000 series and 12000 series. To confirm that a device is not vulnerable to this issue, ensure that ports TCP 5060 and UDP 5060 are not open on the device with the commands **show tcp brief all** and **show ip sockets**. Below is an example of a router running the fixed image c7200-js-mz.124-5b.bin which is **not vulnerable** to this issue.

```
Router#show tcp brief all
```

```
Router#show ip sockets
Proto Remote      Port      Local      Port  In Out Stat TTY OutputIF
```

17 0.0.0.0 0 192.168.100.2 67 0 0 2211 0

No lines with UDP Port 5060 are shown and UDP SIP is not enabled. In this example, UDP port 67 is used by DHCP which is not related to this vulnerability.

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

☐ Details

SIP is a protocol designed for use in IP voice networks and is widely used for Voice over Internet Protocol (VoIP) communications worldwide.

Cisco devices running certain versions of IOS with support for SIP services may be affected by a vulnerability that leads to a reload of the device with a crafted series of SIP packets to either TCP port 5060 or UDP port 5060. This vulnerability affects routers that contain any SIP configuration, including SIP gateways. This issue is being tracked as Cisco Bug ID [CSCsh58082](#) ([registered customers only](#)).

In addition, certain versions of IOS with support for SIP services may process SIP messages even if they are not configured for SIP operation. To process SIP messages IOS will open UDP port 5060 and TCP port 5060 for listening. The Cisco Bug ID that documents the issue of IOS processing SIP messages without being configured for SIP operation is [CSCsb25337](#) ([registered customers only](#)). The fix for this bug turns off the listening ports TCP 5060 and UDP 5060.

A device must have an open SIP port to be vulnerable to this issue. Devices which do not listen on TCP 5060 or UDP 5060 are not vulnerable. Because SIP utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses.

Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS).

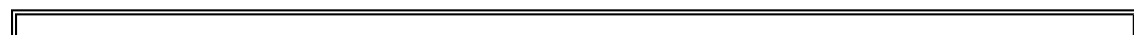
Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided an FAQ to answer additional questions regarding CVSS at <http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at <http://intellishield.cisco.com/security/alertmanager/cvss>.



CSCsb25337 - unnecessary tcp ports opened in default router config Calculate the environmental score of CSCsb25337 ↗						
CVSS Base Score - 2.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Partial	None	None	Normal
Temporal Score - 1.9						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

[CSCsb25337](#) ([registered](#) customers only) causes processing of SIP messages to occur even when an IOS device is not configured for correct SIP operation. The scoring of this bug has been done taking in consideration the potential for reconnaissance since this bug, by itself, has no potential for denial-of-service.

CSCsh58082 - SIP: A router may reload due to SIP traffic (registered customers only) Calculate the environmental score of CSCsh58082 ↗						
CVSS Base Score - 3.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal
Temporal Score - 3.1						
Exploitability		Remediation Level		Report Confidence		
High		Workaround		Confirmed		

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

☐ Impact

Successful exploitation of the vulnerability may result in a reload of the device. The issue may be repeatedly exploited, leading to an extended Denial Of Service (DoS) condition.

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

☐ 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.

Each row of the Cisco IOS software table (below) describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL:
<http://www.cisco.com/warp/public/620/1.html>.

The following table is written to indicate the vulnerable and fixed status of [CSCsh58082](#) ([registered](#) customers only) , which is the bug responsible for the device reload. This table also contains information about IOS releases that are fixed for [CSCsb25337](#) ([registered](#) customers only) , which turns off processing of SIP messages when the device is not fully configured for SIP operation. At the time of the 2.0 publishing, there are no fixes for [CSCsh58082](#) ([registered](#) customers only) .

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Release	Rebuild	Maintenance
12.0	All 12.0 releases are not vulnerable	
Affected 12.1-Based Release	Rebuild	Maintenance
12.1	All 12.1 releases are not vulnerable	
Affected 12.2-Based Release	Rebuild	Maintenance
12.2	All 12.2 releases are not vulnerable	
Affected 12.3-Based Release	Rebuild	Maintenance
12.3	Not vulnerable	
12.3B	Not vulnerable	
12.3BC	Not vulnerable	
12.3BW	Not vulnerable	
12.3JA	Not vulnerable	
12.3JEA	Not vulnerable	
12.3JK	Not vulnerable	

12.3JX	Not vulnerable
12.3T	Vulnerable in all 12.3(8)T and later releases
12.3TPC	Not vulnerable
12.3XA	Not vulnerable
12.3XB	Not vulnerable
12.3XC	Not vulnerable
12.3XD	Not vulnerable
12.3XE	Not vulnerable
12.3XF	Not vulnerable
12.3XG	Not vulnerable
12.3XH	Vulnerable
12.3XI	Not vulnerable
12.3XJ	Not vulnerable
12.3XK	Not vulnerable
12.3XQ	Vulnerable
12.3XR	Vulnerable
12.3XS	Not vulnerable
12.3XU	Vulnerable
12.3XW	SIP ports are closed by default in 12.3(14) YX2 or later, but routers running SIP are still vulnerable
12.3XX	SIP ports are closed by default in 12.3(8) XX2 or later, but routers running SIP are still vulnerable
12.3XY	Vulnerable
12.3YA	Not vulnerable
12.3YD	Not vulnerable
12.3YF	SIP ports are closed by default in 12.3(14) YX2 or later, but routers running SIP are still vulnerable
12.3YG	SIP ports are closed by default in 12.3(8) YG5 or later, but routers running SIP are still vulnerable
12.3YH	Not vulnerable
12.3YI	Not vulnerable
12.3YJ	Not vulnerable

12.3YK	Vulnerable	
12.3YM	SIP ports are closed by default in 12.3(14)YM8 or later, but routers running SIP are still vulnerable	
12.3YQ	Vulnerable	
12.3YS	Not vulnerable	
12.3YT	Vulnerable	
12.3YU	Vulnerable	
12.3YX	SIP ports are closed by default in 12.3(14)YX2 or later, but routers running SIP are still vulnerable	
12.3YZ	Vulnerable	
Affected 12.4-Based Release	Rebuild	Maintenance
12.4	SIP ports are closed by default in a release listed below, but routers running SIP are still vulnerable	
	12.4(3d)	
	12.4(5b)	
	12.4(7a)	12.4(8)
12.4MR	SIP ports are closed by default in 12.4(6)MR or later, but routers running SIP are still vulnerable	
12.4SW	Vulnerable; workaround available for all 12.4SW releases where SIP ports are closed by default	
12.4T	SIP ports are closed by default in a release listed below, but routers running SIP are still vulnerable	
	12.4(2)T5	
	12.4(4)T3	
	12.4(6)T1	12.4(9)T
12.4XA	Vulnerable	
12.4XB	SIP ports are closed by default in 12.4(4)XB2 or later, but routers running SIP are still vulnerable	
12.4XC	SIP ports are closed by default in 12.4(4)XC6* available 12-Feb-07; but routers running SIP are still vulnerable	

12.4XD	SIP ports are closed by default in 12.4(4) XD2 or later, but routers running SIP are still vulnerable
12.4XE	Vulnerable; workaround available for all 12.4XE releases where SIP ports are closed by default
12.4XG	Not vulnerable
12.4XJ	Vulnerable; workaround available for all 12.4XJ releases where SIP ports are closed by default
12.4XP	Vulnerable; workaround available for all 12.4XP releases where SIP ports are closed by default
12.4XT	Vulnerable; workaround available for all 12.4XT releases where SIP ports are closed by default

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

☐ Workarounds

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:
<http://www.cisco.com/warp/public/707/cisco-amb-20070131-sip.shtml>.

Disable SIP listening ports

For devices which do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device with the following commands.

Warning: When applying this workaround to devices which are processing MGCP or H.323 calls, the device will not allow you to 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.

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#sip-ua
Router(config-sip-ua)#no transport udp
Router(config-sip-ua)#no transport tcp
Router(config-sip-ua)#end
```

After applying this workaround the commands **show ip sockets** and **show tcp brief all** will not show the device listening on UDP and TCP port 5060:

```
Router#show ip sockets
Proto  Remote      Port      Local      Port  In  Out  Stat  TTY
  17    --listen--  9.13.32.18  2887      0    0   11   0
```

```
Router#show tcp brief all
TCB          Local Address          Foreign Address      (state)
6649A5A4     *.1720                  *.*                 LISTEN
66CDC764     *.1723                  *.*                 LISTEN
```

Control Plane Policing

For devices which do not need to run SIP, you can use Control Plane Policing (CoPP) to block all SIP access to the device. Cisco IOS software 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 your network.

Warning: Because SIP utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses.

```
!-- Permit all TCP and UDP SIP traffic sent to all IP addresses
!-- configured on all interfaces of the affected device so that it
!-- will be policed and dropped by the CoPP feature.

access-list 100 permit tcp any any eq 5060
access-list 100 permit udp any any eq 5060

!-- 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 drop-sip-traffic
  class drop-sip-class
    drop

!-- Apply the Policy-Map to the Control-Plane of the
!-- device.

control-plane
  service-policy input drop-sip-traffic
```

In the above CoPP example, the access control list entries (ACEs) which 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/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900; and http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlmt.html.

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

☐ **Obtaining Fixed Software**

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

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

☐ **Customers with Service Contracts**

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

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

☐ **Customers using Third Party Support Organizations**

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

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

☐ Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

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

☐ Exploitation and Public Announcements

This issue was first reported to Cisco by a customer. There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

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

☐ Status of this Notice:FINAL

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

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

☐ Distribution

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml>

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

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

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

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

☐ Revision History

Revision 2.1	2007-February-10	Changed formatting and wording of advisory table.
Revision 2.0	2007-February-9	Updated document to reflect that all products with open ports 5060 are vulnerable. Updated Vulnerable Products with voice gateways, SBCs, and CAT6000-CMM. Updated the software table to reflect vulnerability of 12.3(4)XH, 12.3(4)XQ, 12.3(7)XR, 12.3(7)XS, 12.3(8)JA, 12.3(8)XU, 12.3(8)XW, 12.3(8)XX, 12.3(8)XY, 12.3(8)YA, 12.3(8)YH, 12.3(8)YI and 12.3(8)ZA.
Revision 1.1	2007-January-31	Added Common Vulnerability Scoring System (CVSS) scoring for all bugs mentioned in the advisory. Added CSCsh58082 (registered customers only) as the Cisco Bug ID that tracks the root cause of the vulnerability.

		Minor wording changes.
Revision 1.0	2007- January- 31	Initial public release.

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

☐ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

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

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.](#)