

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)

Security Advisories

Cisco Security Advisory: Multiple Product Vulnerabilities Found by PROTOS SIP Test Suite

Advisory ID: [cisco-sa-20030221-protos](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20030221-protos.shtml>

Revision 1.0

For Public Release 2003 February 21 1700 UTC (GMT)

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

Contents

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

Summary

Multiple Cisco products contain vulnerabilities in the processing of Session Initiation Protocol (SIP) INVITE messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for SIP and can be repeatedly exploited to produce a denial of service.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20030221-protos.shtml>.

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

☐ **Affected Products**

This section provides details on affected products.

☐ **Vulnerable Products**

These products are vulnerable:

- Cisco IP Phone Model 7940/7960 running SIP images prior to 4.2
- Cisco Routers running Cisco IOS 12.2T and 12.2 'X' trains
- Cisco PIX Firewall running software versions with SIP support, beginning with version 5.2(1) and up to, but not including versions 6.2(2), 6.1(4), 6.0(4) and 5.2(9)

☐ **Products Confirmed Not Vulnerable**

Cisco products that are not running the SIP protocol or that do not provide Network Address Translation (NAT) fixup services for the SIP protocol are not affected.

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

☐ **Details**

SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based, application-layer control protocol (defined in RFCs 2543 and 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.

The vulnerabilities identified can be easily and repeatedly demonstrated with the use of the OUSPG "PROTOS" Test Suite for SIP. This suite is designed to test the design limits of the implementation of the SIP protocol, specifically the SIP INVITE messages that are used in the initial call setup between two SIP endpoints.

The Cisco IP Phone models 7940 and 7960 are vulnerable to network-based Denial of Service (DoS) attacks via this test suite due to buffer overflows and improper handling of invalid headers. These vulnerabilities are documented as Cisco Bug IDs CSCdz26317, CSCdz29003, CSCdz29033, and CSCdz29041.

Devices running Cisco IOS versions in the 12.2T train or any 12.2 'X' train may reset due to improper handling of SIP fields. These vulnerabilities are documented as Cisco Bug IDs CSCdz39284 and CSCdz41124. In order to be vulnerable to CSCdz39284, the device must be running a vulnerable version of IOS and be configured as a SIP gateway. However, any device running a vulnerable version of Cisco IOS that is configured to perform NAT is vulnerable to CSCdz41124 when SIP is using UDP as its transport.

The Cisco PIX Firewall may reset when receiving fragmented SIP INVITE messages. As the SIP

fixup does not support fragmented SIP messages, this has been resolved to now drop SIP fragments. This vulnerability is documented as Cisco Bug ID CSCdx47789.

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

☐ Impact

Depending on the test case, the Cisco IP Phone models 7940 and 7960 would reset or hang, requiring the manual power cycling of the device.

Vulnerable versions of both Cisco IOS and Cisco PIX Software would experience a device reset.

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

☐ Software Versions and Fixes

Cisco IP SIP Phones

This vulnerability is repaired in Cisco IP Phone SIP Images POS3-04-2-00 and later.

Cisco Secure PIX Firewall

This vulnerability is repaired in Cisco Secure PIX Software versions 5.2.9, 6.0.4, 6.1.4, and 6.2.2 and later.

Cisco IOS

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," "Interim," 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).

When selecting a release, keep in mind the following definitions:

- **Maintenance** - Most heavily tested, stable, and highly recommended release of a release train in any given row of the table.
- **Rebuild** - Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific defect. Although it receives less testing, it contains only the minimal changes necessary to repair the vulnerability.
- **Interim** - Built at regular intervals between maintenance releases and receives less testing. Interims should be selected only if there is no other suitable release that addresses the vulnerability. Interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available through manufacturing, and usually they are not available for customer download from CCO without prior arrangement with the Cisco TAC.

In all cases, customers should exercise caution to confirm that the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new software release. If the information is not clear, contact the Cisco TAC for assistance as shown in the [Obtaining Fixed Software](#) section below.

More information on Cisco IOS software release names and abbreviations is available at <http://www.cisco.com/warp/public/620/1.html>.

The fixes will be available at the Software Center located at <http://www.cisco.com/tacpage/sw-center/>.

Train or Release	Description of Image or Platform	Availability of Fixed Releases		
		Rebuild	Interim	Maintenance
12.2 T		12.2(11) T3 12.2(13) T1		

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

☐ Workarounds

For customers implementing IP Telephony via SIP, there are no known workarounds for most of these defects directly on the devices. The Cisco PSIRT recommends that customers upgrade to a version of software that contains fixes.

However, it may be possible to limit the exposure of SIP-enabled devices by compartmentalizing the traffic to only those segments which require SIP traffic to transit them. This may be done via any traffic-blocking mechanism such as firewalls or router access lists that can block both UDP traffic with source or destination ports of 5060 and TCP traffic with source or destination ports of 5060 and 5061. As always, it is important to investigate whether other local legitimate non-SIP traffic is attempting to use the default ports that SIP may also use before those ports are blocked completely.

Similarly, unless NAT for the SIP protocol is required, devices running vulnerable versions of Cisco IOS which are configured to perform general NAT services may simply implement ingress access lists to prevent the possible translation of the SIP traffic by blocking UDP traffic with source or destination ports of 5060.

Customers running version 6.2 of the Cisco Secure PIX Software may be able to disable the SIP fixup feature depending on the configuration. See the Usage Guidelines section at <http://www.cisco.com/en/US/docs/security/pix/pix63/command/reference/df.html#wp1067379> for more details.

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

☐ Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

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

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

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

☐ Customers with Service Contracts

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

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

☐ Customers using Third Party Support Organizations

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

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

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

☐ Customers without Service Contracts

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

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)

- e-mail: tac@cisco.com

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

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

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

☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any malicious exploitation of these vulnerabilities. This advisory is being published simultaneously with announcements from other organizations such as the CERT Coordination Center.

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

☐ **Status of This Notice: INTERIM**

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

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

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

☐ **Distribution**

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20030221-protos.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
- bugtraq@securityfocus.com
- full-disclosure@lists.netsys.com
- first-teams@first.org (includes CERT/CC)

- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- Various internal Cisco mailing lists

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

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

☐ **Revision History**

Revision 1.0	2003-February-21	Initial public release
--------------	------------------	------------------------

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

☐ **Cisco Security Procedures**

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

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

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

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)



Send

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

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

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)