

Cisco Security Advisory: Cisco Unified IP Phone Overflow and Denial of Service Vulnerabilities

Advisory ID: cisco-sa-20080213-phone

<http://www.cisco.com/warp/public/707/cisco-sa-20080213-phone.shtml>

Revision 1.0

For Public Release 2008 February 13 1600 UTC (GMT)

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

Contents

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

Summary

Cisco Unified IP Phone models contain multiple overflow and denial of service (DoS) vulnerabilities. There are workarounds for several of these vulnerabilities. Cisco has made free software available to address this issue for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080213-phone.shtml>.

☐ **Affected Products**

☐ **Vulnerable Products**

The following Cisco Unified IP Phone devices running Skinny Client Control Protocol (SCCP) firmware:

- 7906G
- 7911G
- 7935
- 7936
- 7940
- 7940G
- 7941G
- 7960
- 7960G
- 7961G
- 7970G
- 7971G

The following Cisco Unified IP Phone devices running Session Initiation Protocol (SIP) firmware:

- 7940
- 7940G
- 7960
- 7960G

The version of firmware running on an IP Phone can be determined via the Settings menu on the phone or via the phone HTTP interface.


☐ **Products Confirmed Not Vulnerable**

No other Cisco products are known to be vulnerable. This includes the following Cisco Unified IP Phone devices:




- 7905
- 7912
- 7921
- 7931
- 7937
- 7942
- 7945
- 7962
- 7965
- 7975

☐ Details

SCCP and SIP-Related Vulnerabilities


- **DNS Response Parsing Overflow**
Cisco Unified IP Phone 7940, 7940G, 7960 and 7960G devices running SCCP and SIP firmware contain a buffer overflow vulnerability in the handling of DNS responses. A specially-crafted DNS response may be able to trigger a buffer overflow and execute arbitrary code on a vulnerable phone. This vulnerability is corrected in SCCP firmware version 8.0(8) and SIP firmware version 8.8(0). This vulnerability is documented in [CVE-2008-0530](#)  and Cisco Bug IDs CSCsj74818 and CSCsk21863.



SCCP-Only Related Vulnerabilities

- **Large ICMP Echo Request DoS**
Cisco Unified IP Phone 7940, 7940G, 7960 and 7960G devices running SCCP firmware contain a DoS vulnerability. It is possible to cause a vulnerable device to reboot by sending a large ICMP echo request packet. This vulnerability is corrected in SCCP firmware version 8.0(6). This vulnerability is documented in [CVE-2008-0526](#)  and Cisco Bug ID CSCsh71110.
- **HTTP Server DoS**
Cisco Unified IP Phone 7935 and 7936 devices running SCCP firmware contain a DoS vulnerability in their internal HTTP server. By sending a specially crafted HTTP request to TCP port 80 on a vulnerable phone, it may be possible to cause the phone to reboot. It is possible to workaround this issue by disabling the internal HTTP server on vulnerable phones. The internal HTTP server only listens to TCP port 80. This vulnerability is corrected in SCCP firmware version 3.2(18) for 7935 devices and SCCP firmware version 3.3(15) for 7936 devices. This vulnerability is documented in [CVE-2008-0527](#)  and Cisco Bug ID CSCsk20026.
- **SSH Server DoS**
Cisco Unified IP Phone 7906G, 7911G, 7941G, 7961G, 7970G and 7971G devices running SCCP firmware contain a buffer overflow vulnerability in their internal Secure Shell (SSH) server. By sending a specially crafted to packet to TCP port 22 on a vulnerable phone, it may be possible for an unauthenticated attacker to cause the phone to reboot. It may also be possible for an unauthenticated attacker to execute arbitrary code with system privileges. It is possible to workaround this issue by disabling the internal SSH server on vulnerable phones. The internal SSH server only listens to TCP port 22. This vulnerability is corrected in SCCP firmware version 8.2(2)SR2. This vulnerability is documented in [CVE-2004-2486](#)  and Cisco Bug ID CSCsh79629.

SIP-Only Related Vulnerabilities

- **SIP MIME Boundary Overflow**
Cisco Unified IP Phone 7940, 7940G, 7960 and 7960G devices running SIP firmware contain a buffer overflow vulnerability in the handling of Multipurpose Internet Mail Extensions (MIME) encoded data. By sending a specially crafted SIP message to a vulnerable phone, it may be possible to trigger a buffer overflow and execute arbitrary code on the phone. This vulnerability is corrected in SIP firmware version 8.8(0). This vulnerability is documented in

[CVE-2008-0528](#)  and Cisco Bug ID CSCsj74786.

- **Telnet Server Overflow**
Cisco Unified IP Phone 7940, 7940G, 7960 and 7960G devices running SIP firmware contain a buffer overflow vulnerability in their internal telnet server. The telnet server is disabled by default and can be configured to allow either privileged or unprivileged user-level access. If the telnet server is enabled for privileged or unprivileged access, the phone password parameter must additionally be configured to permit telnet access. By entering a specially crafted command on a phone configured to permit unprivileged access, it may be possible for an unprivileged-level, authenticated user to trigger a buffer overflow and obtain privileged-level access to the phone. It is possible to work around this issue by disabling the internal telnet server on vulnerable phones. This vulnerability is corrected in SIP firmware version 8.8(0). This vulnerability is documented in [CVE-2008-0529](#)  and Cisco Bug ID CSCsj78359.
- **SIP Proxy Response Overflow**
Cisco Unified IP Phone 7940, 7940G, 7960 and 7960G devices running SIP firmware contain a heap overflow vulnerability in the handling of a challenge/response message from a SIP proxy. If an attacker controls the SIP proxy to which a vulnerable phone is registered, attempts to register, or the attacker can act as a man-in-the-middle, it may be possible to send a malicious challenge/response message to a phone and execute arbitrary code. This vulnerability is corrected in SIP firmware version 8.8(0). This vulnerability is documented in [CVE-2008-0531](#)  and Cisco Bug ID CSCsj74765.

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

☐ Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

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.

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>.

[CSCsj74818 - DNS Response Parsing Stack Overflow](#) (**registered customers only)**

Calculate the environmental score of [CSCsj74818](#)

CVSS Base Score - 10					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - 8.3					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCsk21863 - DNS Response Parsing Stack Overflow (registered customers only)					
Calculate the environmental score of CSCsk21863					
CVSS Base Score - 10					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - 8.3					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCsh71110 - 7940/7960 IP Phone ICMP Denial of Service (registered customers only)					
Calculate the environmental score of CSCsh71110					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCsk20026 - IP Phone HTTP Vulnerability (registered customers only)					
Calculate the environmental score of CSCsk20026					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact

Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

<u>CSCsh79629 - TNP Phone SSH Vulnerability</u> (registered customers only)					
Calculate the environmental score of <u>CSCsh79629</u>					
CVSS Base Score - 10					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - 8.3					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

<u>CSCsj74786 - SIP Mime Boundary Overflow</u> (registered customers only)					
Calculate the environmental score of <u>CSCsj74786</u>					
CVSS Base Score - 10					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - 8.3					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

<u>CSCsj78359 - SIP 40/60:Telnet access stack overflow</u> (registered customers only)					
Calculate the environmental score of <u>CSCsj78359</u>					
CVSS Base Score - 8.5					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	Single	Complete	Complete	Complete
CVSS Temporal Score - 7					
Exploitability		Remediation Level		Report Confidence	

Functional	Official-Fix	Confirmed
------------	--------------	-----------

CSCsj74765 - SIP Proxy Response Overflow (registered customers only)					
Calculate the environmental score of CSCsj74765					
CVSS Base Score - 7.6					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	High	None	Complete	Complete	Complete
CVSS Temporal Score - 6.3					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

☐ Impact

Successful exploitation of these vulnerabilities may cause vulnerable IP phone devices to reboot which will interrupt client voice services and, in some cases, allow the execution of arbitrary code.

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

☐ Software Versions 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.

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

☐ Workarounds

Workarounds are available for several of the vulnerabilities. Disabling unnecessary internal phone Telnet and HTTP servers will eliminate exposure to the Telnet Server overflow and HTTP Server DoS vulnerabilities.

It is possible to mitigate these vulnerabilities with access control lists (ACL). Filters that deny ICMP Echo Request, TCP port 22 (SSH), TCP port 23 (Telnet), TCP port 80 (HTTP), TCP/UDP port 53 (DNS) and TCP/UDP port 5060 (SIP) should be deployed at voice/data network boundaries as part of a tACL policy for protection of traffic which enters the network at ingress access points. This

policy should be configured to protect the network device and other devices behind it where the filter is applied.

Additional information about tACLs is available in "Transit Access Control Lists: Filtering at Your Edge":

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

Additional mitigation techniques 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-20080213-phone.shtml>

[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.

Fixed Firmware for SCCP-Related Vulnerabilities

For the Large ICMP Echo DoS, fixed SCCP firmware version 8.0(6) and later for Cisco Unified IP Phone 7940, 7940G, 7960 and 7960G devices is available.

For the HTTP Server DoS, fixed SCCP firmware version 3.2(18) and later for Cisco Unified IP Phone 7935 devices and fixed SCCP firmware 3.3(15) and later for Cisco Unified IP Phone 7936 devices are available.

For the SSH Server DoS, fixed SCCP firmware version 8.2(2)SR2 and later for Cisco Unified IP Phone 7906G, 7911G, 7941G, 7961G, 7970G and 7971G devices is available.

For the DNS Response Parsing overflow, fixed SCCP firmware version 8.0(8) and later for Cisco Unified IP Phone 7940, 7940G, 7960 and 7960G devices is available.

Fixed firmware for all SCCP-related vulnerabilities can be obtained here:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser?psrtdcat20e2>

Fixed Firmware for SIP-Related Vulnerabilities

All the SIP-related vulnerabilities referenced in this advisory are fixed in SIP firmware version 8.0 (6) and later for Cisco Unified IP Phone 7940, 7940G, 7960 and 7960G devices, which can be obtained here:

<http://www.cisco.com/cgi-bin/tablebuild.pl/sip-ip-phone7960?psrtdcat20e2>

☐ 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>.

☐ 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.

☐ 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 public announcements or malicious use of the vulnerabilities described in this advisory.

The SIP MIME Boundary, Telnet Server, DNS Response Parsing and SIP Proxy Response overflows were reported to Cisco by Jon Griffin and Mustaque Ahamad of the School of Computer Science at the Georgia Institute of Technology.

The HTTP Server DoS was reported to Cisco by Sven Weizenegger of T-Systems.

The Large ICMP Echo Request DoS vulnerability was reported to Cisco by a customer. The SSH Server DoS was discovered internally by Cisco.

[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-20080213-phone.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 1.0	2008-February-13	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.](#)