

Securiteam: [EXPL] Multiple Vulnerabilities in CISCO VoIP Phones (Additional details)

# [EXPL] Multiple Vulnerabilities in CISCO VoIP Phones (Additional details)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0097.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 05/23/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Thu, 23 May 2002 08:59:20 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Multiple Vulnerabilities in CISCO VoIP Phones (Additional details)

---

## SUMMARY

The 7900 line of VoIP phones from Cisco contain remote-accessible code which can be exploited to cause a denial of service, and possibly leak information; the phones are also weak in ways that facilitate man-in-the-middle attacks directed at intercepting telephone traffic. Vulnerable products include CP-7960, CP-7940, and CP-7910 phones.

For ways of protecting yourself from this vulnerability see our previous article: <http://www.securiteam.com/securitynews/5VP0M0K75S.html>  
Multiple Vulnerabilities in Cisco IP Telephones.

## DETAILS

Vulnerabilities:

1. The Cisco 7900 series of phones include a built-in web server on port 80. The server provides several pages of debug and status information about the phone and is presumably intended for diagnostic purposes. However the pages require no authentication and some are CGI scripts with exploitable errors. The most glaring of these is the StreamingStatistics page. Opening <http://>/StreamingStatistics?1> will present a page of debug statistics as intended. Requesting statistics on a non-existent

stream, e.g. <http://>/StreamingStatistics?7> will return a page indicating the error. However, requesting statistics for a stream with sufficiently high ID will cause a hard-reset of the phone.

Testing has produced varying results, but hard reset tends to occur with IDs > 32768, and using an (arbitrarily selected) ID of 120000 consistently produces the reset. This results in a reboot process of approximately 15–30 seconds during which the phone is not in service. The result is a very simple and not at all packet intensive DoS possibility. The attack is further facilitated the phone's willingness to provide its IP and phone number through the web page, allowing an attacker to walk a subnet looking for the correct IP, when targeting a specific extension.

2. Related to #1, another script on the phone's website, PortInformation has similar, though less catastrophic input validation problems. It uses the same format as above, <http://>/PortInformation?1> will give you information on the first Ethernet port of the phone (which has its own port, as well as a second 10/100 switched port for connecting a computer to the network without requiring multiple Ethernet drops).

Like StreamingStatistics, PortInformation will indicate an invalid port number up to a point (again, results vary, but IDs over 32768 seem to cause the problem consistently). Above that limit, rather than crashing, the page is generated with what looks like the contents of arbitrary memory locations. It is conceivable that a dedicated attacker could put this data to some use. If a tool were developed which could extract from this, for instance, the phone's recent calls lists, then it would be possible for an intruder to monitor and map telephone usage within the system. This is certainly not as dangerous as #1, but it should clearly be fixed nonetheless.

3. The telephones store all of their network information locally and most of it is accessible through the "Settings" button on the phone. By default, these settings are locked (as indicated by a padlock icon when viewing them) however the key to unlock the settings is the constant string '\* \* \* #' (entered from the phone's keypad).

This is not admin-configurable. Once unlocked, several fields can be specified, including the TFTP server from which the phone receives its configuration file. Among other things, this file provides the phone with the list of CallManager IPs who will provide the telephony services. With one-time physical access to the phone, an attacker could enter an alternate, malicious TFTP server which would provide the phone with attacker-controlled CallManager IPs.

In this fashion, the attacker could route all telephone traffic through his or her systems, presumably recording it or altering it before passing it to the legitimate CallManager systems for transport. This modification of the phone's configuration is very unlikely to be noticed, since a user never has to interact with the network settings menu where these changes were made.

Securiteam: [EXPL] Multiple Vulnerabilities in CISCO VoIP Phones (Additional details)

Vendor Status:

Cisco first contacted March 27, 2002 and responded promptly. They have released an advisory that can be found at:

<<http://www.securiteam.com/securitynews/5VP0M0K75S.html>> Multiple Vulnerabilities in Cisco IP Telephones.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:johnath@johnath.com>> Johnathan Nightingale.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[TOOL] boegADT, Automated Exploit Code Generation"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)