

# [NEWS] Cisco Unified IP Conference Station and IP Phone Vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00076.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 22 Feb 2007 13:47:05 +0200
- 

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Cisco Unified IP Conference Station and IP Phone Vulnerabilities

---

## SUMMARY

Certain Cisco Unified IP Conference Station and IP Phone devices contain vulnerabilities which may allow unauthorized users to gain administrative access to vulnerable devices.

## DETAILS

Cisco Unified IP Conference Station Administrative Bypass Vulnerability  
Cisco Unified IP Conference Station 7935 and 7936 devices do not require a password when a URL is accessed directly via the administrator HTTP interface. There is a workaround for this vulnerability.

Cisco Unified IP Phone Default Account and Privilege Escalation Vulnerabilities

Cisco Unified IP Phone 7906G, 7911G, 7941G, 7961G, 7970G and 7971G devices contain a hard coded default user account with a default password which is remotely accessible via a Secure Shell (SSH) server enabled on the phone. This default user account may be leveraged to gain administrative access to a vulnerable phone via a privilege escalation vulnerability. The default user account may also execute commands causing a phone to become

## [NEWS] Cisco Unified IP Conference Station and IP Phone Vulnerabilities

unstable and result in a denial of service. The default user account can not be disabled, removed or have its password changed. There are mitigations available for these vulnerabilities.

Cisco has made free software available to address these issues for affected customers.

### Products Confirmed Not Vulnerable

Cisco Unified IP Phone 7902G, 7905, 7905G, 7910, 7912, 7912G, 7920, 7921G, 7940, 7960 and 7985 devices are not vulnerable to the default account and privilege escalation vulnerability.

No other Cisco products are known to be vulnerable.

### Details

#### Cisco Unified IP Conference Station Administrative Bypass Vulnerability

Cisco Unified IP Conference Station 7935 and 7936 devices provide integrated speaker phone services for a networked environment. 7935/7936 devices can be managed via an administrative HTTP interface and/or a with Cisco Unified CallManager (CUCM) system. The administrative HTTP interface is protected by a user configurable password. If a user knows the direct path to a management URL, it may be possible to access the administrative HTTP interface without being prompted for authentication. The vulnerability occurs because vulnerable IP Conference Station devices incorrectly maintain the state of administrator login sessions. If an administrator logs into a vulnerable device via the HTTP interface, the administrator's credentials will be cached even after the administrator logs out of the device. This leaves a window of opportunity for an unauthorized user to gain complete administrative access to a vulnerable device. If an administrator never accesses a potentially vulnerable device via the HTTP interface, the device is not vulnerable to the authentication bypass attack. It is possible to reset to an IP Conference Station to a non-vulnerable state by power-cycling the device or performing a reboot operation (not a reload operation) via the CUCM system which manages the device. This defect is documented in Cisco Bug ID [CSCsg26788](http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg26788) ( registered customers only) .

#### Cisco Unified IP Phone Default Account and Privilege Escalation Vulnerabilities

Cisco Unified IP Phone 7906G, 7911G, 7941G, 7961G, 7970G and 7971G devices provide integrated phone service for a networked environment. These IP phones devices contain a hard coded default user account with a default password that is used for debugging purposes and is embedded into the phone's firmware. This default user account cannot be disabled, removed or have its password changed. Due to an implementation error, it possible to use the hard coded default user account to remotely access the Command Line Interface (CLI) of a vulnerable IP phone via a phone's SSH server. The SSH server is only supposed to authenticate user accounts which have been created by an administrator. The SSH server may not be disabled. The firmware update including the solution for this vulnerability prohibits

## [NEWS] Cisco Unified IP Conference Station and IP Phone Vulnerabilities

the default user account from accessing a phone via the SSH server, but the default user account may still access the phone via the console serial port. This defect is documented in Cisco Bug ID

<<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg34758>>  
CSCsg34758 ( registered customers only) .

Using the default user account to access the CLI of a vulnerable IP phone device (via SSH or the console serial port), an attacker can execute a number of commands which may result in the escalation of privileges leading to complete compromise of an affected IP phone or cause an IP phone to become unstable and crash. These defects are documented in Cisco Bug IDs

<<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg34789>>  
CSCsg34789 ( registered customers only) and

<<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg42627>>  
CSCsg42627 ( registered customers only) .

### Impact:

Successful exploitation of the Conference Station administrative bypass or IP Phone default account and privilege escalation vulnerabilities may result in the complete compromise of a vulnerable device.

### Workarounds:

For Cisco Unified Conference Station and IP Phone devices, the following mitigations have been provided.

The effectiveness of any mitigation 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 mitigation or fix is the most appropriate for use in the intended network before it is deployed.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document for this advisory:

<<http://www.cisco.com/warp/public/707/cisco-air-20070221-phone.shtml>>  
<http://www.cisco.com/warp/public/707/cisco-air-20070221-phone.shtml>

Apply access control lists (ACLs) on routers, switches and firewalls that filter traffic to vulnerable Conference Station and IP Phone devices so that traffic is only allowed from stations that need to remotely administer the devices.

It is possible to workaround the Cisco Unified IP Conference Station Administrative Bypass vulnerability by ensuring that the administrative HTTP interface is not used to manage any vulnerable devices. If the HTTP interface must be used, vulnerable devices should be power cycled or rebooted via a CUCM system after system changes are made.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:psirt@xxxxxxxx>> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20070221-phone.shtml>>

<http://www.cisco.com/warp/public/707/cisco-sa-20070221-phone.shtml>

=====

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@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

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

=====

=====

**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.