

Cisco Security Advisory: Cisco Unified IP Conference Station and IP Phone Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-02/msg00392.html>

- *From:* Cisco Systems Product Security Incident Response Team <psirt@xxxxxxxx>
 - *Date:* Thu, 21 Feb 2007 17:09:11 -0000
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Cisco Security Advisory: Cisco Unified IP Conference Station and IP Phone Vulnerabilities

Advisory ID: cisco-sa-20070221-phone

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

Revision 1.0

For Public Release 2007 February 21 1600 UTC (GMT)

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.

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

Cisco Security Advisory: Cisco Unified IP Conference Station and IP Phone Vulnerabilities

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 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.

This advisory is posted at
<http://www.cisco.com/warp/public/707/cisco-sa-20070221-phone.shtml>

Affected Products

=====

This section provides details on affected products.

Vulnerable Products

+-----

This section provides details on vulnerable products.

Cisco Unified IP Conference Station

+-----

+-----+

| Model | Affected Firmware Version |

|-----|

| 7935 | 3.2(15) and earlier |

|-----|

| 7936 | 3.3(12) and earlier |

+-----+

Cisco Unified IP Phone

+-----

+-----+

| Model | Firmware Version |

|-----|

| 7906G | 8.0(4)SR1 and earlier |

|-----|

| 7911G | 8.0(4)SR1 and earlier |

|-----|

| 7941G | 8.0(4)SR1 and earlier |

|-----|

| 7961G | 8.0(4)SR1 and earlier |

|-----|

| 7970G | 8.0(4)SR1 and earlier |

|-----|

| 7971G | 8.0(4)SR1 and earlier |

+-----+

Cisco Security Advisory: Cisco Unified IP Conference Station and IP Phone Vulnerabilities

The version of firmware running on an IP phone can be determined via the Settings menu on a phone.

In most deployments, Cisco Unified CallManager (CUCM) can also be used to accurately determine the version of firmware that is supposed to be running on an IP phone. While CUCM maintains a record of the firmware it last deployed to an IP phone, it is possible for a user to change the firmware version on an IP phone.

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 (registered customers only) .

Cisco Unified IP Phone Default Account and Privilege Escalation Vulnerabilities

+-----

Cisco Security Advisory: Cisco Unified IP Conference Station and IP Phone 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 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 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 CSCsg34789 (registered customers only) and CSCsg42627 (registered customers only) .

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>

CSCsg26788 – IP Conference Station HTTP Interface Administrator Bypass

CVSS Base Score: 10
Access Vector: Remote
Access Complexity: Low
Authentication: Not Required
Confidentiality Impact: Complete
Integrity Impact: Complete
Availability Impact: Complete
Impact Bias: Normal

CVSS Temporal Score: 8.3
Exploitability: Functional
Remediation Level: Official Fix
Report Confidence: Confirmed

CSCsg34758 – IP Phone SSH Vulnerability

CVSS Base Score: 10
Access Vector: Remote
Access Complexity: Low
Authentication: Not Required
Confidentiality Impact: Complete
Integrity Impact: Complete
Availability Impact: Complete
Impact Bias: Normal

CVSS Temporal Score: 8.3
Exploitability: Functional
Remediation Level: Official Fix
Report Confidence: Confirmed

CSCsg34789 – Filesystem Privilege Escalation

CVSS Base Score: 6
Access Vector: Remote
Access Complexity: Low
Authentication: Required
Confidentiality Impact: Complete
Integrity Impact: Complete
Availability Impact: Complete
Impact Bias: Normal

CVSS Temporal Score: 5
Exploitability: Functional
Remediation Level: Official Fix
Report Confidence: Confirmed

CSCsg42627 – Filesystem Denial of Service

CVSS Base Score: 2
Access Vector: Remote
Access Complexity: Low
Authentication: Required
Confidentiality Impact: None
Integrity Impact: None
Availability Impact: Complete
Impact Bias: Normal

CVSS Temporal Score: 1.7
Exploitability: Functional
Remediation Level: Official Fix
Report Confidence: Confirmed

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.

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.

Cisco Unified IP Conference Station
+-----

Model	Fixed Firmware Version
7935	3.2(16)
7936	3.3(13)

Cisco Unified IP Phone

```
+-----+
+-----+
| Model | Fixed Firmware Version |
+-----+
| 7906G | 8.0(4)SR2, 8.2(1) |
+-----+
| 7911G | 8.0(4)SR2, 8.2(1) |
+-----+
| 7941G | 8.0(4)SR2, 8.2(1) |
+-----+
| 7961G | 8.0(4)SR2, 8.2(1) |
+-----+
| 7970G | 8.0(4)SR2, 8.2(1) |
+-----+
| 7971G | 8.0(4)SR2, 8.2(1) |
+-----+
```

Fixed software can be obtained here:

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

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>

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.

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@xxxxxxxx" or "security-alert@xxxxxxxx" for software upgrades.

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@xxxxxxxxxx

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.

Exploitation and Public Announcements

=====

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

The Conference Station administrative bypass vulnerability was reported to Cisco by Christian Reichert, Christian Blum and Jens Link of Intact Integrated Services.

The IP Phone default account and privilege escalation vulnerabilities were discovered internally by Cisco.

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.

Distribution

=====

Cisco Security Advisory: Cisco Unified IP Conference Station and IP Phone Vulnerabilities

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

<http://www.cisco.com/warp/public/707/cisco-sa-20070221-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@xxxxxxxxx
- * first-teams@xxxxxxxxx
- * bugtraq@xxxxxxxxxxxxxxxxxxxxx
- * vulnwatch@xxxxxxxxxxxxxxxxx
- * cisco@xxxxxxxxxxxxxxxxxxxxx
- * cisco-nsp@xxxxxxxxxxxxxxxxxxxxx
- * full-disclosure@xxxxxxxxxxxxxxxxxxxxx
- * comp.dcom.sys.cisco@xxxxxxxxxxxxxxxxxxxxx

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.

Revision History

=====

Revision	Initial
1.0	2007-February-21 public release

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>.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.5 (Darwin)

iD8DBQFF3Hvp8NUAbBmDaxQRAnvdAJ9QxYW2cOJ3l0wWMkX6HEK1/Vh4+gCfZDpg
Wd3DU9Ni70fR69GAF5ht5GU=

=zd0p

-----END PGP SIGNATURE-----