

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of Cisco Unified IP Conference Station and IP Phone Vulnerabilities

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

Revision 1.0

For Public Release 2007 February 21 1600 UTC (GMT)

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

Contents

[Cisco Response](#)
[Device-Specific Mitigation and Identification](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)
[Related Information](#)

Cisco Response

Vulnerability Characteristics

The Cisco Unified IP Conference Station and IP Phone devices contain the following vulnerabilities:

1. It may be possible to access the Unified IP Conference Station administrative HTTP interface without authentication. This vulnerability can be exploited remotely with no authentication and no user interaction. If exploited, the attacker may alter the device configuration or create a Denial of Service. In a default configuration the attack vector is through TCP port 80. The TCP port used by the HTTP interface is configurable and should be verified before any traffic filtering is added to the network. This vulnerability is not designated by a CVE ID.
2. Vulnerable Cisco Unified IP Phones contain a default username and password that may be accessed via SSH. This vulnerability can be exploited remotely with no user interaction. If exploited, the attacker may be able to modify the device configuration or perform additional attacks. The attack vector is through TCP port 22. This vulnerability is not designated by a CVE ID.
3. Affected Cisco Unified IP Phones contain privilege escalation vulnerabilities that allow local, authenticated users to obtain administrative access to the phone. This vulnerability may be exploited remotely with authentication and no user interaction. If exploited, the attacker may be able to modify the device configuration or cause a Denial of Service. The attack vector is through TCP port 22. This vulnerability is not designated by a CVE ID.

The privilege escalation vulnerabilities involve defects in the command line interface of the affected devices. Upgrading vulnerable devices to fixed software is the only effective means by which to mitigate these particular vulnerabilities; therefore, no identification or mitigation techniques for these vulnerabilities will be detailed in this document.

This document contains information to assist Cisco customers in mitigating attempts to exploit the Cisco Unified IP Conference Station and IP Phone Vulnerabilities.

Vulnerable, non-affected and fixed software information is available in the PSIRT Security Advisory:

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

Mitigation Technique Overview

Cisco devices provide several countermeasures for the Administrative Bypass and Default Account Vulnerabilities. The most preventive control is provided by IOS and PIX, ASA, and FWSM Firewall Access Control Lists (ACLs) at the network level. Detective controls can also be performed by IOS devices and PIX, ASA, and FWSM Firewalls through syslog messages and Access Control List show commands. The configuration of ACLs to protect voice devices is a security best practice.

More information about securing Unified Communications can be obtained in the Voice Security section of the Unified Communications Solution Reference Network Design (SRND) for CallManager [4.x](#) or [5.x](#). The network connectivity (i.e. ports and protocols) needed for the various versions of CallManager can be obtained at [Cisco CallManager TCP and UDP Port Usage](#).

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

Device-Specific Mitigation and Identification

Specific information on mitigation and identification is available for these platforms and devices:

- [Cisco ASA, PIX and FWSM Firewalls](#)
- [Cisco IOS Switches and Routers](#)

Cisco ASA, PIX and FWSM Firewalls

Mitigation: Administrative Bypass and Default Account Vulnerabilities

Access Control Lists

Access Control Lists (ACLs) on Cisco ASA, PIX and FWSM Firewalls are an effective means to block traffic traversing the network. ACLs should be constructed and placed in order to protect vulnerable devices. ACLs are typically placed on existing policy enforcement points closest to the devices to be protected.

The following ACL permits traffic on TCP port 22 and TCP port 80 from trusted sources (192.168.1.0/24) to the vulnerable devices (10.1.1.0/24). All other TCP port 22 and TCP port 80 traffic is explicitly denied.

```

!
!-- Permit TCP port 22 (ssh) and TCP port 80 (www) from trusted sources only
!
access-list ACL-OUTSIDE-IN extended permit tcp 192.168.1.0 255.255.255.0
10.1.1.0 255.255.255.0 eq 22
access-list ACL-OUTSIDE-IN extended permit tcp 192.168.1.0 255.255.255.0
10.1.1.0 255.255.255.0 eq 80
access-list ACL-OUTSIDE-IN extended deny tcp any 10.1.1.0 255.255.255.0 eq 22
access-list ACL-OUTSIDE-IN extended deny tcp any 10.1.1.0 255.255.255.0 eq 80
!
!-- Permit or deny other traffic in accordance with existing security policies.
!
!-- Apply ACL to ingress interfaces.
!
access-group ACL-OUTSIDE-IN in interface outside
!

```

Identification: Administrative Bypass and Default Account Vulnerabilities

Access Control List Hit Counters

The **show access-list** command displays the contents of each ACL. Additionally, this command will display the number of packets matching each Access Control Entry (ACE).

The example shown below indicates 61 TCP port 22 (ssh) packets and 25 TCP port 80 (www) packets from sources not explicitly trusted have been denied by this ACL.

```

Firewall#show access-list
access-list ACL-OUTSIDE-IN; 4 elements
access-list ACL-OUTSIDE-IN line 1 extended permit tcp 192.168.1.0
255.255.255.0 10.1.1.0 255.255.255.0 eq ssh (hitcnt=0)
access-list ACL-OUTSIDE-IN line 2 extended permit tcp 192.168.1.0
255.255.255.0 10.1.1.0 255.255.255.0 eq www (hitcnt=0)
access-list ACL-OUTSIDE-IN line 3 extended deny tcp any 10.1.1.0
255.255.255.0 eq ssh (hitcnt=61)
access-list ACL-OUTSIDE-IN line 4 extended deny tcp any 10.1.1.0
255.255.255.0 eq www (hitcnt=25)
Firewall#

```

Syslog Messages

The Cisco ASA, PIX and FWSM Firewalls will create a syslog message with ID 106023 for packets denied by ACEs without the log keyword. The following is a sample message.

```

Feb 05 2007 06:36:54: %FWSM-4-106023: Deny tcp src outside:172.16.1.2/4608
dst inside:10.1.1.2/80 by access-group
"ACL-OUTSIDE-IN" [0x722cd9e2, 0x0]

```

More information about the syslog messages created by the Cisco ASA, PIX and FWSM Firewalls can be obtained at:

- FWSM Firewall version 2.x:
<http://www.cisco.com/en/US/docs/security/fwsm/fwsm23/system/message/fsmmsgs.html>
- FWSM Firewall version 3.1:
<http://www.cisco.com/en/US/docs/security/fwsm/fwsm31/system/message/logmsgs.html>
- PIX Firewall 7.x and ASA Security Appliance:
<http://www.cisco.com/en/US/docs/security/asa/asa72/system/message/logmsgs.html>

Cisco IOS Switches and Routers

Mitigation: Administrative Bypass and Default Account Vulnerabilities

Access Control Lists

Use Access Control Lists on Cisco IOS devices to restrict SSH and HTTP access to the affected devices. Outbound ACLs are the most effective means to restrict traffic destined for the networks containing vulnerable devices. The following ACL allows TCP port 22 and TCP port 80 from trusted sources only; all other TCP traffic on ports 22 and 80 is explicitly denied.

```

!
!-- Permit TCP port 22 and TCP port 80 traffic from trusted sources only
!
ip access-list extended ACL-UC-OUT
 permit tcp 192.168.1.0 0.0.0.255 10.1.1.0 0.0.0.255 eq 22
 permit tcp 192.168.1.0 0.0.0.255 10.1.1.0 0.0.0.255 eq 80
 deny tcp any 10.1.1.0 0.0.0.255 eq 22
 deny tcp any 10.1.1.0 0.0.0.255 eq 80
!
!-- Permit or deny other traffic in accordance with existing security policies.
!
!-- Apply outbound ACL to interfaces facing vulnerable devices.
!
interface Vlan 100
 description *** Voice VLAN ***
 ip address 10.1.1.1 255.255.255.0
 ip access-group ACL-UC-OUT out
!

```

Transit ACLs (tACLs) may also be used as an effective mitigation technique for the Administrative Bypass and Default Account Vulnerabilities. tACLs will provide effective mitigation from attacks that transit enforcement points.

For more information on transit ACLs, refer to [Transit Access Control Lists: Filtering at Your Edge](#).

Identification: Administrative Bypass and Default Account Vulnerabilities

Access Control List Hit Counters

The **show access-list** command will display the number of packets matching each ACE. The sample output below illustrates an ACL in which 27 TCP port 22 (ssh) packets and 42 TCP port 80 (www) packets have been denied.

```

switch#show access-list ACL-UC-OUT
Extended IP access list ACL-UC-OUT
 10 permit tcp 192.168.1.0 0.0.0.255 10.1.1.0 0.0.0.255 eq 22
 20 permit tcp 192.168.1.0 0.0.0.255 10.1.1.0 0.0.0.255 eq www
 30 deny tcp any 10.1.1.0 0.0.0.255 eq 22 (27 matches)
 40 deny tcp any 10.1.1.0 0.0.0.255 eq www (42 matches)
switch#

```

ACL Logging

The **log** or **log-input** ACL option will cause packets matching specific ACEs to be logged. The **log-input** option

enables logging of the ingress interface in addition to the packet source and destination IP addresses and ports.

Note: Access Control List logging can be very CPU intensive and must be used with extreme caution.

The CPU impact from ACL Logging is driven by two factors; process switching as a result of packets matching log enabled ACEs and log generation and transmission.

The CPU impact from ACL logging can be addressed in hardware on the Catalyst 6500 Switches and Cisco 7600 Routers with Supervisor 720 and Supervisor 32 using [Optimized ACL Logging](#) or [Hardware Rate Limiting](#).

The **ip access-list logging interval** *interval-in-msec* command can limit the affects of ACL logging-induced process switching. The **logging rate-limit** *rate-per-second* **except** *loglevel* command limits the impact of log generation and transmission.

The configuration below illustrates logging best practices in addition to the **ip access-list logging interval** and **logging rate-limit** commands. The **ip access-list logging interval 60000** command limits log-induced software processing to one packet per source per 60 seconds (60,000 msec). The **logging rate-limit 20 except 4** command shown below limits log generation and transmission to 20 messages per second except for log levels 4 and below.

```

!
service timestamps log datetime msec
!
logging on
no logging console
no logging monitor
logging buffered informational
logging buffered 16386
logging rate-limit 20 except 4
logging <syslog-host>
!
ip access-list logging interval 60000
!

```

The following ACL has been updated to include logging of TCP port 22 and TCP port 80 packets from those sources not specifically trusted.

```

!
!-- Permit TCP ports 22 and 80 from trusted sources only
!
ip access-list extended ACL-UC-OUT
 permit tcp 192.168.1.0 0.0.0.255 10.1.1.0 0.0.0.255 eq 22
 permit tcp 192.168.1.0 0.0.0.255 10.1.1.0 0.0.0.255 eq 80
 deny tcp any 10.1.1.0 0.0.0.255 eq 22 log-input
 deny tcp any 10.1.1.0 0.0.0.255 eq 80 log-input
!
!-- Permit the remaining traffic in accordance with existing security policies.
!
!-- Apply outbound ACL to interface.
!
interface Vlan 100
 description *** Voice VLAN ***
 ip address 10.1.1.1 255.255.255.0
 ip access-group ACL-UC-OUT out
!

```

Log messages will be generated for packets matching logging enabled ACEs. The following is a sample of such a message. Using the command **show log | include IPACCESSLOGP** will limit the output to ACL Logging.

```
Switch#show log | in IPACCESSLOGP
Feb  2 05:57:35.016: %SEC-6-IPACCESSLOGP: list ACL-UC-OUT denied tcp
172.16.1.2(4600) (Vlan250 000d.607b.1e19) ->
10.1.1.2(22), 1 packet
```

Additional Information

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.

Revision History

Revision 1.0	2007-February-21	Initial 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>.

Related Information

- [Catalyst 6500 Optimized ACL Logging](#)
- [FWSM 2.x Syslog Messages](#)
- [FWSM 3.1 Syslog Messages](#)
- [IOS Command Reference 'logging rate-limit'](#)
- [PIX/ASA 7.2 Syslog Messages](#)
- [Ports and Protocol by CallManager Version](#)
- [Unified Communications Solution Reference Network Design \(SRND\) for CallManager 4.x](#)
- [Unified Communications Solution Reference Network Design \(SRND\) for CallManager 5.x](#)

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)

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

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

© 2009 - 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)