Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager IP Phone Personal Address Book Synchronizer Privilege Escalation Vulnerability

Document ID: 109446

http://www.cisco.com/warp/public/707/cisco−amb−20090311−cucmpab.shtml

Revision 1.0

For Public Release 2009 March 11 1600 UTC (GMT)

Please provide your feedback on this document.

Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisory *Cisco Unified Communications Manager IP Phone Personal Address Book Synchronizer Privilege Escalation Vulnerability* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

The Cisco Unified Communications Manager contains a privilege escalation vulnerability in the IP Phone Personal Address Book Synchronizer feature. This vulnerability can be exploited remotely with authentication and without end−user interaction. Successful exploitation of this vulnerability may allow information disclosure, which enables an attacker to learn information about the affected device or network. The attack vector for exploitation is through TCP packets using ports 8404 and 8405.

This vulnerability has been assigned CVE identifier CVE−2009−0632.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory, which is available at the following link:
http://www.cisco.com/warp/public/707/cisco−sa−20090311−cucmpab.shtml.

Mitigation Technique Overview

Cisco devices provide several countermeasures for this vulnerability. Administrators are advised to consider these protection methods to be general security best practices for infrastructure devices and the traffic that transits the network. This section of the document provides an overview of these techniques.

Cisco IOS Software can provide effective means of exploit prevention using infrastructure access control lists (iACLs). This protection mechanism filters and drops packets that are attempting to exploit this vulnerability.

Effective exploit prevention can also be provided by the Cisco ASA 5500 Series Adaptive Security Appliance, the Cisco PIX 500 Series Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers using transit access control lists (tACLs). This protection mechanism filters and drops packets that are attempting to exploit this vulnerability.

Cisco IOS NetFlow flow records can provide visibility into network−based exploitation attempts.

Cisco IOS Software, Cisco ASA appliances, Cisco PIX security appliances, and FWSM firewalls can provide visibility through syslog messages and the counter values displayed in the output from **show** commands.

Risk Management

Organizations are advised to follow their standard risk evaluation and mitigation processes to determine the potential impact of this vulnerability. Triage refers to sorting projects and prioritizing efforts that are most likely to be successful. Cisco has provided documents that can help organizations develop a risk−based triage capability for their information security teams. Risk Triage for Security Vulnerability Announcements and Risk Triage and Prototyping can help organizations develop repeatable security evaluation and response processes.

Device Specific Mitigation and Identification

Caution: The effectiveness of any mitigation technique is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. As with any configuration change, evaluate the impact of this configuration prior to applying the change.

Specific information about mitigation and identification is available for these devices:

- Cisco IOS Routers and Switches
- Cisco IOS NetFlow
- Cisco ASA, PIX, and FWSM Firewalls

Cisco IOS Routers and Switches

Mitigation: Infrastructure Access Control Lists

To protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators are advised to deploy infrastructure access control lists (iACLs) to perform policy enforcement of traffic sent to infrastructure equipment. Administrators can construct an iACL by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. For the maximum protection of infrastructure devices, deployed iACLs should be applied in the ingress direction on all interfaces to which an IP address has been configured. An iACL workaround cannot provide complete protection against this vulnerability when the attack originates from a trusted source

address.

The iACL policy denies unauthorized packets on TCP ports 8404 and 8405 that are sent to affected devices. In the following example, 192.168.60.0/24 is the IP address space that is used by the affected devices, and the host at 192.168.100.1 is considered a trusted source that requires access to the affected devices. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic. Whenever possible, infrastructure address space should be distinct from the address space used for user and services segments. Using this addressing methodology will assist with the construction and deployment of iACLs.

Additional information about iACLs is in Protecting Your Core: Infrastructure Protection Access Control Lists.

```
ip access-list extended Infrastructure-ACL-Policy

!
 !-- When applicable, include explicit permit statements for trusted
 !-- sources that require access on the vulnerable ports
 !

 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8404
 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8405

!
 !-- The following vulnerability-specific access control entries
 !-- (ACEs) can aid in identification of attacks
 !

 deny tcp any 192.168.60.0 0.0.0.255 eq 8404
 deny tcp any 192.168.60.0 0.0.0.255 eq 8405

!
 !-- Explicit deny ACE for traffic sent to addresses configured within
 !-- the infrastructure address space
 !

 deny ip any 192.168.60.0 0.0.0.255

!
 !-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
 !-- with existing security policies and configurations
 !
!-- Apply iACL to interfaces in the ingress direction
!

interface GigabitEthernet0/0
 ip access-group Infrastructure-ACL-Policy in

!
```

Note that filtering with an interface access list will elicit the transmission of ICMP unreachable messages back to the source of the filtered traffic. Generating these messages could have the undesired effect of increasing CPU utilization on the device. In Cisco IOS Software, ICMP unreachable generation is limited to one packet every 500 milliseconds by default. ICMP unreachable message generation can be disabled using the interface configuration command **no ip unreachables**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable** *interval-in-ms*.

Identification: Infrastructure Access Control Lists

After the administrator applies the iACL to an interface, the **show ip access−lists** command will identify the number of packets on TCP port 8404 and 8405 that have been filtered on interfaces on which the iACL is applied. Administrators should investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show ip access−lists Infrastructure−ACL−Policy** follows:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
    10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8404
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8405
    30 deny tcp any 192.168.60.0 0.0.0.255 eq 8404 (11 matches)
    40 deny tcp any 192.168.60.0 0.0.0.255 eq 8405 (12 matches)
    50 deny ip any 192.168.60.0 0.0.0.255
router#
```

In the preceding example, access list *Infrastructure−ACL−Policy* has dropped the following packets that are received from an untrusted host or network:

- **11** packets on **TCP port 8404** for ACE line 30
- **12** packets on **TCP port 8405** for ACE line 40

For additional information about investigating incidents using access control entry (ACE) counters and syslog events, reference the Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence white paper.

Administrators can use Embedded Event Manager to provide instrumentation when specific conditions are met, such as ACE counter hits. The Applied Intelligence white paper Embedded Event Manager in a Security Context provides additional details about how to use this feature.

Identification: Access List Logging

The **log** and **log−input** access control list (ACL) option will cause packets that match 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.

Caution: Access control list logging can be very CPU intensive and must be used with extreme caution. Factors that drive the CPU impact of ACL logging are log generation, log transmission, and process switching to forward packets that match log−enabled ACEs.

For Cisco IOS Software, the **ip access−list logging interval** *interval−in−ms* command can limit the effects of process switching induced by ACL logging. The **logging rate−limit** *rate−per−second* [**except** *loglevel*] command limits the impact of log generation and transmission.

The CPU impact from ACL logging can be addressed in hardware on the Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers with Supervisor Engine 720 or Supervisor Engine 32 using optimized ACL logging.

For additional information about the configuration and use of ACL logging, reference the Understanding Access Control List Logging Applied Intelligence white paper.

Cisco IOS NetFlow

Identification: Traffic Flow Identification Using NetFlow Records

Administrators can configure Cisco IOS NetFlow on Cisco IOS routers and switches to aid in the identification of traffic flows that may be attempts to exploit the vulnerability. Administrators are advised to investigate flows to determine whether they are attempts to exploit the vulnerability or whether they are legitimate traffic flows.

```
router#show ip cache flow
IP packet size distribution (899 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .466 .533 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  70 active, 4026 inactive, 152 added
  1701 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25800 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-WWW              7      0.0        10    40      0.2       0.0      15.5
TCP-other           34      0.1         5    40      0.6       0.0      15.5
UDP-DNS              5      0.0         3    28      0.0       0.0      15.3
UDP-other           36      0.1         5    28      0.5       0.0      15.4
Total:              82      0.2         5    34      1.4       0.0      15.4

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.182.38  Et0/1         192.168.242.157 11 1271 971F     5
Et0/0         192.168.207.55  Et0/1         192.168.60.116  06 B006 20D4     8
Et0/0         192.168.207.167 Et0/1         192.168.50.167  06 0CE1 9564     6
Et0/0         192.168.254.35  Et0/1         192.168.135.137 06 83D0 D5EA     1
Et0/0         192.168.245.243 Et0/1         192.168.162.249 11 C236 37D2    15
Et0/0         192.168.240.255 Et0/1         192.168.60.12   06 F61D 20D4    15
Et0/0         192.168.121.1   Et0/1         192.168.163.143 11 0631 E75F    18
Et0/0         192.168.10.71   Et0/1         192.168.60.187  06 9CBE 20D4     2
Et0/0         192.168.123.142 Et0/1         192.168.235.40  11 88D1 E045     4
Et0/0         192.168.42.31   Et0/1         192.168.60.28   06 CFCA 20D4     7
Et0/0         192.168.124.169 Et0/1         192.168.125.179 11 D401 50F7     2
Et0/0         192.168.197.222 Et0/1         192.168.147.179 06 1C45 1CA3     2
Et0/0         192.168.150.65  Et0/1         192.168.123.147 11 8470 4AA8     5
Et0/0         192.168.103.120 Et0/1         192.168.10.227  06 F6B8 9CDB    14
Et0/0         192.168.41.80   Et0/1         192.168.41.104  11 F057 15D8     5
Et0/0         192.168.14.166  Et0/1         192.168.89.196  11 37F6 2065     3
Et0/0         192.168.151.200 Et0/1         192.168.73.48   06 1C7E 1436     5
Et0/0         192.168.203.72  Et0/1         192.168.60.84   06 E80D 20D5     5
Et0/0         192.168.64.245  Et0/1         192.168.163.175 06 18E8 F39A     5
Et0/0         192.168.225.245 Et0/1         192.168.60.159  06 9107 20D5     2
Et0/0         192.168.130.51  Et0/1         192.168.44.150  11 CD43 EAB3    16
Et0/0         192.168.222.66  Et0/1         192.168.69.14   06 4634 BAC2     5
Et0/0         192.168.165.231 Et0/1         192.168.7.113   11 AB05 3686     4
Et0/0         192.168.145.180 Et0/1         192.168.166.137 06 C80B 871D     5
Et0/0         192.168.237.193 Et0/1         192.168.3.183   11 147E DD8E     5
Et0/0         192.168.129.142 Et0/1         192.168.139.39  06 7EA1 5C04     5
Et0/0         192.168.85.66   Et0/1         192.168.149.92  11 1DA6 AE44     5
Et0/0         192.168.192.195 Et0/1         192.168.22.152  11 4001 CD50     6
```

```
Et0/0         192.168.113.134 Et0/1         192.168.60.120  06 C3B3 20D4     9
Et0/0         192.168.181.89  Et0/1         192.168.60.201  06 4C4C 20D4     4
Et0/0         192.168.15.165  Et0/1         192.168.60.149  11 C8FD 36C7    10
Et0/0         192.168.110.97  Et0/1         192.168.169.168 11 A592 10BF     6
Et0/0         192.168.192.244 Et0/1         192.168.108.161 11 27C4 3041     5
Et0/0         192.168.122.82  Et0/1         192.168.56.204  06 1DB3 7B26     1
Et0/0         192.168.157.31  Et0/1         192.168.126.176 11 E093 7FF9     5
Et0/0         192.168.201.52  Et0/1         192.168.184.25  11 1ED3 EC86     3
Et0/0         192.168.163.28  Et0/1         192.168.60.249  06 245D 20D4     1
router#
```

In the preceding example, there are multiple flows for **TCP** ports **8404 (hex value 20D4)** and **8405 (hex value 20D5)**.

To view only the traffic flows for packets on TCP ports 8404 (hex value 20D4) and 8405 (hex value 20D5), the command **show ip cache flow | include SrcIf|_06_.*(20D4|20D5)_** will display the related TCP NetFlow records as shown here:

```
router#show ip cache flow | include SrcIf|_06_.*(20D4|20D5)_
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.21.55   Et0/1         192.168.60.149  06 6AC9 20D4     8
Et0/0         192.168.111.179 Et0/1         192.168.60.2    06 119F 20D4     7
Et0/0         192.168.208.124 Et0/1         192.168.60.176  06 840B 20D5     5
Et0/0         192.168.134.164 Et0/1         192.168.60.142  06 5BA2 20D4     1
Et0/0         192.168.102.126 Et0/1         192.168.60.143  06 FD1B 20D4     1
Et0/0         192.168.253.177 Et0/1         192.168.60.252  06 4714 20D5     2
Et0/0         192.168.177.16  Et0/1         192.168.60.117  06 8E8A 20D5     5
Et0/0         192.168.63.179  Et0/1         192.168.60.234  06 D7CE 20D4    13
router#
```

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Transit Access Control Lists

To protect the network from traffic that enters the network at ingress access points, which may include Internet connection points, partner and supplier connection points, or VPN connection points, administrators are advised to deploy tACLs to perform policy enforcement. Administrators can construct a tACL by explicitly permitting only authorized traffic to enter the network at ingress access points or permitting authorized traffic to transit the network in accordance with existing security policies and configurations. A tACL workaround cannot provide complete protection against this vulnerability when the attack originates from a trusted source address.

The tACL policy denies unauthorized packets on TCP ports 8404 and 8405 that are sent to affected devices. In the following example, 192.168.60.0/24 is the IP address space that is used by the affected devices, and the host at 192.168.100.1 is considered a trusted source that requires access to the affected devices. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic.

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

```
!
!-- Include any explicit permit statements for trusted sources
!-- that require access on the vulnerable ports
!

access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0
```

```
!
!-- The following vulnerability-specific access control entries
!-- (ACEs) can aid in identification of attacks
!

access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8404
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8405

!
!-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Explicit deny for all other IP traffic
!

access-list tACL-Policy extended deny ip any any

!
!-- Apply tACL to interface(s) in the ingress direction
!

access-group tACL-Policy in interface outside
```

Identification: Transit Access Control Lists

After the tACL has been applied to an interface, administrators can use the **show access-list** command to identify the number of packets on TCP ports 8404 and 8405 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show access-list tACL-Policy** follows:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 5 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1 192.168.60.0 255.255
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1 192.168.60.0 255.255
access-list tACL-Policy line 3 extended deny tcp any 192.168.60.0 255.255.255.0 eq 8404 (h
access-list tACL-Policy line 4 extended deny tcp any 192.168.60.0 255.255.255.0 eq 8405 (h
access-list tACL-Policy line 5 extended deny ip any any (hitcnt=20)
firewall#
```

In the preceding example, access list *tACL-Policy* has dropped the following packets received from an untrusted host or network:

- **19** packets on **TCP port 8404** for ACE line 3
- **143** packets on **TCP port 8405** for ACE line 4

Identification: Firewall Access List Syslog Messages

Firewall syslog message *106023* will be generated for packets denied by an access control entry (ACE) that does not have the **log** keyword present. Additional information about this syslog message is in Cisco Security Appliance System Log Message - 106023.

Information about configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or the Cisco PIX 500 Series Security Appliance is in Monitoring the Security Appliance - Configuring and Managing Logs. Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is in Monitoring the Firewall Services Module.

In the following example, the **show logging | grep** *regex* command extracts syslog messages from the logging buffer on the firewall. These messages provide additional information about denied packets that could indicate potential attempts to exploit the vulnerability that is described in this document. It is possible to use different

regular expressions with the **grep** keyword to search for specific data in the logged messages.

Additional information about regular expression syntax is in Creating a Regular Expression.

```
firewall#show logging | grep 106023
Dec 31 2008 12:56:18: %ASA-4-106023: Deny tcp src outside:192.168.21.38/55625 dst
   inside:192.168.60.213/8404 by access-group "tACL-Policy"
Jan 01 2009 11:15:20: %ASA-4-106023: Deny tcp src outside:192.168.244.207/52045 dst
   inside:192.168.60.210/8404 by access-group "tACL-Policy"
Jan 01 2009 19:53:17: %ASA-4-106023: Deny tcp src outside:192.168.24.36/7772 dst
   inside:192.168.60.160/8404 by access-group "tACL-Policy"
Jan 02 2009 05:34:39: %ASA-4-106023: Deny tcp src outside:192.168.108.51/5785 dst
   inside:192.168.60.228/8404 by access-group "tACL-Policy"
Jan 02 2009 19:14:01: %ASA-4-106023: Deny tcp src outside:192.168.15.37/45991 dst
   inside:192.168.60.37/8405 by access-group "tACL-Policy"
Jan 03 2009 02:45:08: %ASA-4-106023: Deny tcp src outside:192.168.8.220/61502 dst
   inside:192.168.60.65/8405 by access-group "tACL-Policy"
Jan 03 2009 04:48:27: %ASA-4-106023: Deny tcp src outside:192.168.89.125/41317 dst
   inside:192.168.60.32/8405 by access-group "tACL-Policy"
Jan 03 2009 22:20:12: %ASA-4-106023: Deny tcp src outside:192.168.146.115/23012 dst
   inside:192.168.60.150/8405 by access-group "tACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *tACL−Policy* show packets for **TCP ports 8404 and 8405** sent to the address block assigned to affected devices.

Additional information about syslog messages for ASA and PIX security appliances is in Cisco Security Appliance System Log Messages. Additional information about syslog messages for the FWSM is in Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging System Log Messages.

For additional information about investigating incidents using syslog events, reference the Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence white paper.

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	2009−MAR−11	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

- **Cisco Applied Mitigation Bulletins**
- **Cisco Guide to Harden Cisco IOS Devices**
- **Cisco Security Center**
- **Cisco IOS NetFlow − Home Page on Cisco.com**
- **Cisco IOS NetFlow White Papers**
- **NetFlow Performance Analysis**
- **Cisco Network Foundation Protection White Papers**
- **Cisco Network Foundation Protection Presentations**
- **A Security−Oriented Approach to IP Addressing**
- **Cisco Firewall Products − Home Page on Cisco.com**

Contacts & Feedback | Help | Site Map © 2008 − 2009 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Mar 11, 2009 Document ID: 109446
