

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)

Applied Mitigation Bulletins

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager CTL Provider Heap Overflow

<http://www.cisco.com/warp/public/707/cisco-amb-20080116-cucmctl.shtml>

Revision 1.0

For Public Release 2008 January 16 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

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisory *Cisco Unified Communications Manager CTL Provider Heap Overflow* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

The Cisco Unified Communications Manager (CUCM) Cisco Certificate Trust List (CTL) Provider service contains a vulnerability when it processes specially crafted TCP packets. This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may allow arbitrary code execution or result in a denial of service (DoS) condition. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack

vector for exploitation is through CTL Provider services packets using TCP port 2444, which is the default port for this service. This port value will be used for the examples in this document. If the port has been changed from the default value of 2444, then the example access list policies and IPS signature will need to be modified to the configured port value for the CTL Provider service.

This vulnerability has been assigned CVE identifier CVE-2008-0027.

Note: The CTL Provider service port is operator configurable and can be verified within the CUCM user-interface (UI) as explained in the following steps:

1. Choose **System > Service Parameters**.
2. Choose the **Server Name** from the drop-down list.
3. Choose **Cisco CTL Provider** from the **Service** drop-down list.

The term *Inactive* or *Active* appended to the service name in the list signifies whether the service is enabled or disabled. When the **Cisco CTL Provider** service is selected, the port number value for the *CTL Provider* service is displayed in the **Parameters** box. This port number will be used for the *CTL Provider* service when it is enabled.

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-20080116-cucmctl.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 Transit access control lists (tACLs).

This protection mechanism filters and drops packets that are attempting to exploit the vulnerability that has a network attack vector.

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 the vulnerability that has a network attack vector.

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

Cisco IOS Software, Cisco ASA, 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 depends 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.

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

Cisco IOS Routers and Switches

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 transit access control lists (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 the vulnerability that has a network attack vector when the attack comes from a trusted source address.

The tACL policy denies unauthorized CTL Provider Service packets on TCP port 2444 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 available in [Transit Access Control Lists: Filtering at Your Edge](#).

```
!-- Include any explicit permit statements for trusted sources
!-- that require access on the vulnerable port
!
access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 2444
!
!-- The following vulnerability-specific access control entries
!-- (ACEs) can aid in identification of attacks
!
```

```

access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 2444

!
!-- 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 150 deny ip any any

!
!-- Apply tACL to interfaces in the ingress direction

interface GigabitEthernet0/0
 ip access-group 150 in

!

```

Note: 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 may result in the undesirable effect of increased 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 unreachable**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable interval-in-ms**.

Identification: Transit Access Control Lists

After the administrator applies the tACL to an interface, the **show ip access-lists** command will identify the number of CTL Provider service packets on TCP port 2444 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 ip access-lists 150** follows:

```

router#show ip access-lists 150
Extended IP access list 150
 10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 2444 (37 matches)
 20 deny tcp any 192.168.60.0 0.0.0.255 eq 2444 (67 matches)
 30 deny ip any any (300 matches)
router#

```

In the preceding example, access list 150 has dropped **67 CTL Provider service** packets on **TCP port 2444** for ACE sequence ID 20.

For additional information about investigating incidents using ACE counters and Syslog Events, reference the [Identifying Incidents Using Firewall and IOS Router Syslog Events](#) Applied Intelligence white paper.

Embedded Event Manager can be utilized 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 on how to utilize this feature.

Identification: Access List Logging

The **log** or **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, as described in this document, that has a network attack vector. 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 (90784136 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

  512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
  .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
1885 active, 63651 inactive, 59960004 added
129803821 aged polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
0 active, 16384 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-Telnet       11393421    2.8         1     48    3.1      0.0     1.4
TCP-FTP           236         0.0         12    66    0.0      1.8     4.8
```

TCP-FTPD	21	0.0	13726	1294	0.0	18.4	4.1
TCP-WWW	22282	0.0	21	1020	0.1	4.1	7.3
TCP-X	719	0.0	1	40	0.0	0.0	1.3
TCP-BGP	1	0.0	1	40	0.0	0.0	15.0
TCP-Frag	70399	0.0	1	688	0.0	0.0	22.7
TCP-other	47861004	11.8	1	211	18.9	0.0	1.3
UDP-DNS	582	0.0	4	73	0.0	3.4	15.4
UDP-NTP	287252	0.0	1	76	0.0	0.0	15.5
UDP-other	310347	0.0	2	230	0.1	0.6	15.9
ICMP	11674	0.0	3	61	0.0	19.8	15.5
IPv6INIP	15	0.0	1	1132	0.0	0.0	15.4
GRE	4	0.0	1	48	0.0	0.0	15.3
Total:	59957957	14.8	1	196	22.5	0.0	1.5

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.11.131	Gi0/1	192.168.60.245	06	0B66	098C	18
Gi0/0	192.168.10.201	Gi0/1	192.168.60.102	11	0984	00A1	1
Gi0/0	192.168.1.230	Gi0/1	192.168.60.42	06	0C09	098C	23
Gi0/0	192.168.11.54	Gi0/1	192.168.60.158	11	0911	00A1	3
Gi0/0	192.168.12.110	Gi0/1	192.168.60.163	06	092A	098C	35
Gi0/1	192.168.150.60	Gi0/0	10.89.16.226	06	0016	12CA	1
Gi0/0	192.168.13.97	Gi0/1	192.168.60.28	11	0B3E	00A1	5
Gi0/0	192.168.11.230	Gi0/1	192.168.60.20	06	0C09	098C	72
Gi0/0	192.168.10.17	Gi0/1	192.168.60.97	11	0B89	00A1	1
Gi0/0	192.168.72.110	Gi0/1	192.168.60.118	06	092A	098C	44
Gi0/0	10.88.226.1	Gi0/1	192.168.202.22	11	007B	007B	1
Gi0/0	192.168.13.7	Gi0/1	192.168.60.162	06	0914	098C	21
Gi0/0	192.168.12.185	Gi0/1	192.168.60.239	11	0BD7	00A1	1
Gi0/0	192.168.41.86	Gi0/1	192.168.60.27	06	0B7B	098C	11
Gi0/0	10.89.16.226	Gi0/1	192.168.150.60	06	12CA	0016	1

router#

In the preceding example, there are multiple flows for **CTL Provider service** on **TCP port 2444 (hex value 098C)**. Administrators are advised to compare these flows to baseline utilization for CTL Provider service traffic sent on TCP port 2444 and to investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for **CTL Provider service** packets on **TCP port 2444 (hex value 098C)**, the command **show ip cache flow | include SrcIf|_06_.*098C** will display the related NetFlow records as shown in the following example:

```
router#show ip cache flow | include SrcIf|_06_.*098C
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.12.110	Gi0/1	192.168.60.163	06	092A	098C	35
Gi0/0	192.168.72.110	Gi0/1	192.168.60.118	06	092A	098C	44
Gi0/0	192.168.11.230	Gi0/1	192.168.60.20	06	0C09	098C	72
Gi0/0	192.168.1.230	Gi0/1	192.168.60.42	06	0C09	098C	23
Gi0/0	192.168.11.131	Gi0/1	192.168.60.245	06	0B66	098C	18
Gi0/0	192.168.13.7	Gi0/1	192.168.60.162	06	0914	098C	21
Gi0/0	192.168.41.86	Gi0/1	192.168.60.27	06	0B7B	098C	11

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 the vulnerability that has a network attack vector when the attack comes from a trusted source address.

The tACL policy denies unauthorized CTL Provider service packets on TCP port 2444 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 available in [Transit Access Control Lists: Filtering at Your Edge](#).

```

!
!-- Include any explicit permit statements for trusted sources
!-- requiring access on the vulnerable port
!

access-list Transit-ACL-Policy extended permit tcp host
    192.168.100.1 192.168.60.0 255.255.255.0 eq 2444

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

access-list Transit-ACL-Policy extended deny tcp any
    192.168.60.0 255.255.255.0 eq 2444

!
!-- 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 Transit-ACL-Policy extended deny ip any any

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

access-group Transit-ACL-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 CTL Provider service packets on TCP port 2444 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to

exploit this vulnerability. The following example shows output for **show access-list Transit-ACL-Policy**:

```
firewall#show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 3 elements
access-list Transit-ACL-Policy line 1 extended permit tcp host
 192.168.100.1 192.168.60.0 255.255.255.0 eq 2444 (hitcnt=137)
access-list Transit-ACL-Policy line 2 extended deny tcp any
 192.168.60.0 255.255.255.0 eq 2444 (hitcnt=98)
access-list Transit-ACL-Policy line 3 extended deny ip any any (hitcnt=387)
firewall#
```

In the preceding example, access list *Transit-ACL-Policy* has dropped **98 CTL Provider service** packets on **TCP port 2444** received from an untrusted host or network. In addition, syslog message *106023* can provide valuable information, which includes the source and destination IP address, the source and destination port numbers, and the IP protocol for the denied packet.

For additional information about investigating incidents using ACE counters and Syslog Events, reference the [Identifying Incidents Using Firewall and IOS Router Syslog Events](#) Applied Intelligence white paper.

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 available 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 available in [Configuring Logging on the Cisco Security Appliance](#). Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available in [Configuring Monitoring and Logging on the Cisco FWSM](#).

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 described in this document that has a network attack vector. 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 available in [Using the Command Line Interface](#).

```
firewall#show logging | grep 106023
Dec 19 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.18/2944 dst
 inside:192.168.60.191/2444 by access-group "Transit-ACL-Policy"
Dec 19 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.3.200/2945 ds
 inside:192.168.60.33/2444 by access-group "Transit-ACL-Policy"
Dec 19 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.99/2946 dst
 inside:192.168.60.240/2444 by access-group "Transit-ACL-Policy"
Dec 19 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.100/2947 ds
 inside:192.168.60.115/2444 by access-group "Transit-ACL-Policy"
Dec 19 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.4.88/2949 dst
 inside:192.168.60.38/2444 by access-group "Transit-ACL-Policy"
Dec 19 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.3.175/2950 ds
```

```
inside:192.168.60.250/2444 by access-group "Transit-ACL-Policy"  
firewall#
```

In the preceding example, the messages logged for the tACL *Transit-ACL-Policy* show **CTL Provider service** packets for **TCP port 2444** which have been received from an untrusted host or network.

For additional information about investigating incidents using ACE counters and 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	2008-January-16	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](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Cisco IOS NetFlow - Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco Network Foundation Protection Presentations](#)
- [Understanding Access Control List Logging](#)
- [Embedded Event Manager in a Security Context](#)
- [Identifying Incidents Using Firewall and IOS Router Syslog Events](#)
- [A Security-Oriented Approach to IP Addressing](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Common Vulnerabilities and Exposures \(CVE\)](#)

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)

Send

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).