

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco Unified Communications Web-Based Management Vulnerability

Document ID: 99696

<http://www.cisco.com/warp/public/707/cisco-amb-20071017-IPCC.shtml>

Revision 1.1

Last Updated 2007 October 23 0230 UTC (GMT)

For Public Release 2007 October 22 2215 UTC (GMT)

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

[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 Web-Based Management Vulnerability* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

The Cisco Unified Communications Manager Web-Based Management interface contains an authorization vulnerability for users with valid credentials. This vulnerability could allow a valid, but unauthorized user privileged access to the web-based reporting and scripting tool and administrative access to the web-based configuration tool. This vulnerability can be exploited remotely with authentication and without end-user interaction. The attack vector for exploitation is through HTTP using TCP port 80 and HTTPS using TCP port 443.

Successful exploitation of this vulnerability may allow information disclosure, which could enable an attacker to learn information about the affected device. Exploitation may also allow the attacker to change configurations. This vulnerability has been assigned CVE name CVE-2007-5539.

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-20071017-IPCC.shtml>.

Mitigation Technique Overview

Cisco devices provide several countermeasures for the web-based management 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.

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 described in this document.

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 described in this document.

Cisco IOS NetFlow can provide visibility into these 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 should 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 in Information Security Engagements](#) 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: Transit Access Control Lists

In an effort to protect the network from traffic that enters at ingress access points, which may include Internet connection points, partner and supplier connection points, or VPN connection points, administrators should 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.

The tACL policy denies unauthorized HTTP packets on TCP port 80 and HTTPS packets on TCP port 443 sent to affected devices. In the following example, 192.168.1.0/24 is the network IP address space 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 ports

access-list 150 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq www
access-list 150 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 443

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

access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq www
access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq 443

!--- 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 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 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 HTTP packets on TCP port 80 and HTTPS packets on TCP port 443 that have been filtered. Administrators should 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 192.168.100.1 192.168.1.0 0.0.0.255 eq www
```

```

20 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 443
30 deny tcp any 192.168.1.0 0.0.0.255 eq www (12 matches)
40 deny tcp any 192.168.1.0 0.0.0.255 eq 443 (10 matches)
50 deny ip any any
router#

```

In the preceding example, access list 150 has dropped **12 HTTP** packets on **TCP** port **80** for ACE sequence ID 30 and **10 HTTPS** packets on **TCP** port **443** for ACE sequence ID 40.

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.

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 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.

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 described in this document. Administrators should investigate flows to determine whether they are attempts to exploit this 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

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	192.168.10.201	Gi0/1	192.168.1.102	06	3984	0050	1
Gi0/0	192.168.11.54	Gi0/1	192.168.1.158	06	1111	01BB	3
Gi0/1	192.168.150.60	Gi0/0	10.89.16.226	06	0016	12CA	1
Gi0/0	192.168.13.97	Gi0/1	192.168.1.28	06	843E	0050	5
Gi0/0	192.168.10.17	Gi0/1	192.168.1.97	06	8089	01BB	1
Gi0/0	10.88.226.1	Gi0/1	192.168.202.22	11	007B	007B	1
Gi0/0	192.168.12.185	Gi0/1	192.168.1.239	06	27D7	0050	1
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 **HTTP** on **TCP** port **80** (hex value **0050**) and **HTTPS** on **TCP** port **443** (hex value **01BB**). Administrators should compare these flows to baseline utilization for HTTP traffic sent on TCP port 80 and HTTPS traffic sent on TCP port 443 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows to addresses in the 192.168.1.x subnet for HTTP packets on TCP ports 80 (hex value 0050) and HTTPS packets on TCP port 443 (hex value 01BB), the command **show ip cache flow | include SrcIf|192\168\1\.*_06_.*(0050|01BB)** will display the related NetFlow records as shown here:

```
router#show ip cache flow | include SrcIf|192\168\1\.*_06_.*(0050|01BB)
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.12.110	Gi0/1	192.168.1.163	06	392A	0050	6
Gi0/0	192.168.11.230	Gi0/1	192.168.1.20	06	1109	01BB	1
Gi0/0	192.168.11.131	Gi0/1	192.168.1.245	06	8456	01BB	18
Gi0/0	192.168.13.7	Gi0/1	192.168.1.162	06	2720	01BB	1
Gi0/0	192.168.41.86	Gi0/1	192.168.1.27	06	1193	0050	2

router#

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Transit Access Control Lists

In an effort to protect the network from traffic that enters at ingress access points, which may include Internet connection points, partner and supplier connection points, or VPN connection points, administrators should 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.

The tACL policy denies unauthorized HTTP packets on TCP port 80 and HTTPS packets on TCP port 443 sent to affected devices. In the following example, 192.168.1.0/24 is the network IP address space 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 ports

access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0 eq www
access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0 eq https

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

access-list Transit-ACL-Policy extended deny tcp any 192.168.1.0 255.255.255.0 eq www
access-list Transit-ACL-Policy extended deny tcp any 192.168.1.0 255.255.255.0 eq https

!--- 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 interfaces 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 HTTP packets on TCP port 80 and HTTPS packets on TCP port 443 that have been filtered. Administrators should investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show access-list Transit-ACL-Policy** follows:

```
firewall#show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 5 elements
access-list Transit-ACL-Policy line 1 extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0 eq www
access-list Transit-ACL-Policy line 2 extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0 eq https
access-list Transit-ACL-Policy line 3 extended deny tcp any 192.168.1.0 255.255.255.0 eq www
access-list Transit-ACL-Policy line 4 extended deny tcp any 192.168.1.0 255.255.255.0 eq https
access-list Transit-ACL-Policy line 5 extended deny ip any any (hitcnt=8)
firewall#
```

In the preceding example, the access list Transit-ACL-Policy has dropped **20 HTTP** packets on **TCP port 80** and **11 HTTPS** packets on **TCP port 443** 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.

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 attempts to exploit the vulnerability 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 available in [Using the Command Line Interface](#).

```
firewall#show logging | grep 106023
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.2.118/1923 dst
inside:192.168.1.201/443 by access-group "Transit-ACL-Policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.3.211/4045 dst
inside:192.168.1.13/80 by access-group "Transit-ACL-Policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.2.199/8567 dst
inside:192.168.1.140/80 by access-group "Transit-ACL-Policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.2.100/1809 dst
inside:192.168.1.15/80 by access-group "Transit-ACL-Policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.4.188/6768 dst
inside:192.168.1.138/443 by access-group "Transit-ACL-Policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.3.115/4876 dst
inside:192.168.1.50/443 by access-group "Transit-ACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *Transit-ACL-Policy* show **HTTP** and **HTTPS** packets on **TCP** port **80** and **443** sent to the address block assigned to the network infrastructure.

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

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 1.1	2007-October-23	Include assigned CVE names
Revision 1.0	2007-October-17	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](#)
 - [Understanding Access Control List Logging](#)
 - [Cisco IOS NetFlow – Home Page on Cisco.com](#)
 - [Cisco IOS NetFlow White Papers](#)
 - [Cisco Network Foundation Protection White Papers](#)
 - [Cisco Network Foundation Protection Presentations](#)
 - [Cisco Firewall Products – Home Page on Cisco.com](#)
 - [Common Vulnerabilities and Exposures \(CVE\)](#)
-

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

Updated: Oct 23, 2007

Document ID: 99696
