Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco Wireless LAN Controllers

http://www.cisco.com/warp/public/707/cisco-amb-20090727-wlc.shtml

Revision 1.0

For Public Release 2009 July 27 1600 UTC (GMT)

Please provide your feedback on this document.

Contents

Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisory *Multiple Vulnerabilities in Cisco Wireless LAN Controllers* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

There are multiple vulnerabilities in Cisco Wireless LAN Controllers. The following subsections summarize these vulnerabilities:

Malformed HTTP or HTTPS authentication response denial of service vulnerability: This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability

may cause the affected device to reload resulting in a denial of service (DoS) condition. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition.

The attack vectors for exploitation are through packets using the following protocols and ports:

- HTTP using TCP port 80
- HTTPS using TCP port 443

This vulnerability has been assigned CVE identifier CVE-2009-1164.

SSH connections denial of service vulnerability: This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may cause the affected device to reload resulting 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 SSH packets using TCP port 22.

This vulnerability has been assigned CVE identifier CVE-2009-1165.

Crafted HTTP or HTTPS request denial of service vulnerability: This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may cause the affected device to crash resulting in a denial of service (DoS) condition. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition.

The attack vectors for exploitation are through packets using the following protocols and ports:

- HTTP using TCP port 80
- HTTPS using TCP port 443

This vulnerability has been assigned CVE identifier CVE-2009-1166.

Crafted HTTP or HTTPS request unauthorized configuration modification vulnerability: This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may allow arbitrary code execution, result in a denial of service (DoS) condition, or allow information disclosure, which enables an attacker to learn information about the affected device.

The attack vectors for exploitation are through packets using the following protocols and ports:

- HTTP using TCP port 80
- HTTPS using TCP port 443

This vulnerability has been assigned CVE identifier CVE-2009-1167.

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-20090727-wlc.shtml.

Mitigation Technique Overview

Cisco devices provide several countermeasures for these vulnerabilities. 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 these vulnerabilities.

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 these vulnerabilities.

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 these vulnerabilities. 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.

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

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 these vulnerabilities when the attack originates from a trusted source address.

The tACL policy denies unauthorized packets that are sent to affected devices via the following protocols:

- Secure Shell (SSH) using TCP port 22
- HTTP using TCP port 80
- HTTPS using TCP port 443

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 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq
22
access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq
80
access-list 150 permit tcp host 192.168.100.1 192.168.60.0 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 192.168.60.0 0.0.0.255 eq 22
access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 80
access-list 150 deny tcp any 192.168.60.0 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 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: Transit Access Control Lists

After the administrator applies the tACL to an interface, the **show ip access-lists** command will identify the number of SSH packets on TCP port 22, HTTP packets on TCP port 80, and HTTPS packets on TCP port 443 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit these vulnerabilities. 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 22
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 80
    30 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
    40 deny tcp any 192.168.60.0 0.0.0.255 eq 22 (19 matches)
    50 deny tcp any 192.168.60.0 0.0.0.255 eq 80 (71 matches)
    60 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (34 matches)
    70 deny ip any any
router#
```

In the preceding example, access list 150 has dropped the following packets that are received from an untrusted host or network:

- **19 SSH** packets on **TCP port 22** for ACE line 40
- **71 HTTP** packets on **TCP port 80** for ACE line 50
- **34 HTTPS** packets on **TCP port 443** for ACE line 60

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.

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 these vulnerabilities. Administrators are advised to investigate flows to determine whether they are attempts to exploit these vulnerabilities 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 ager 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         192.168.10.221  Gi0/1         192.168.60.112  06 0984
0016     7
Gi0/0         192.168.11.34   Gi0/1         192.168.60.128  06 0911
0050    21
Gi0/0         192.168.10.21   Gi0/1         192.168.60.12   11 0984
007B     7
Gi0/0         192.168.10.16   Gi0/1         192.168.60.11   06 0984
0016    11
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    11 0016
12CA     3
Gi0/0         192.168.13.86   Gi0/1         192.168.60.18   06 0B3E
01BB     5
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  11 12CA
0016    11
Gi0/0         192.168.11.33   Gi0/1         192.168.60.17   06 0911
0050    61
Gi0/0         192.168.13.66   Gi0/1         192.168.60.8    06 0B3E
01BB     9
router#
```

In the preceding example, there are multiple flows for **SSH** packets on **TCP** port **22 (hex value 0016)**, **HTTP** packets on **TCP** port **80 (hex value 0050)**, and **HTTPS** packets on **TCP** port **443 (hex value 01BB)**.

To view only the traffic flows for SSH packets on TCP port 22 (hex value 0016), HTTP packets on TCP port 80 (hex value 0050), and HTTPS packets on TCP port 443 (hex value 01BB), the command **show ip cache flow | include SrcIf|_06_.*(0016|0050|01BB)_** will display the related TCP NetFlow records as shown here:

```
router#show ip cache flow | include SrcIf|_06_.*(0016|0050|01BB)_
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP
DstP  Pkts
Gi0/0         192.168.10.221  Gi0/1         192.168.60.112  06 0984
0016     7
Gi0/0         192.168.11.34   Gi0/1         192.168.60.128  06 0911
0050    21
Gi0/0         192.168.10.16   Gi0/1         192.168.60.11   06 0984
0016    11
Gi0/0         192.168.13.86   Gi0/1         192.168.60.18   06 0B3E
01BB     5
Gi0/0         192.168.11.33   Gi0/1         192.168.60.17   06 0911
0050    61
Gi0/0         192.168.13.66   Gi0/1         192.168.60.8    06 0B3E
01BB     9
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 these vulnerabilities when the attack originates from a trusted source address.

The tACL policy denies unauthorized packets that are sent to affected devices via the following protocols:

- Secure Shell (SSH) using TCP port 22
- HTTP using TCP port 80
- HTTPS using TCP port 443

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 eq 22
access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 80
access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 443

!
!-- 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 22
access-list tACL-Policy extended deny tcp any 192.168.60.0
255.255.255.0 eq 80
access-list tACL-Policy extended deny tcp any 192.168.60.0
255.255.255.0 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 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 SSH packets on TCP port 22, HTTP packets on TCP port 80, and HTTPS packets on TCP port 443 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit these vulnerabilities. Example output for **show access-list tACL-Policy** follows:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 7 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq ssh (hitcnt=27)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
```

```
192.168.60.0 255.255.255.0 eq www (hitcnt=97)
access-list tACL-Policy line 3 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq https (hitcnt=51)
access-list tACL-Policy line 4 extended deny tcp any 192.168.60.0
255.255.255.0 eq ssh (hitcnt=11)
access-list tACL-Policy line 5 extended deny tcp any 192.168.60.0
255.255.255.0 eq www (hitcnt=127)
access-list tACL-Policy line 6 extended deny tcp any 192.168.60.0
255.255.255.0 eq https (hitcnt=101)
access-list tACL-Policy line 7 extended deny ip any any (hitcnt=210)
firewall#
```

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

- **11 SSH** packets on **TCP port 22** for ACE line 4
- **127 HTTP** packets on **TCP port 80** for ACE line 5
- **101 HTTPS** packets on **TCP port 443** for ACE line 6

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 vulnerabilities that are 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
  Jun 21 2009 00:15:13: %ASA-4-106023: Deny tcp src
outside:192.0.2.18/2944
         dst inside:192.168.60.191/22 by access-group "tACL-Policy"
  Jun 21 2009 00:15:13: %ASA-4-106023: Deny tcp src
outside:192.2.0.200/2945
         dst inside:192.168.60.33/22 by access-group "tACL-Policy"
  Jun 21 2009 00:15:13: %ASA-4-106023: Deny tcp src
outside:192.0.2.99/2946
         dst inside:192.168.60.240/80 by access-group "tACL-Policy"
  Jun 21 2009 00:15:13: %ASA-4-106023: Deny tcp src
outside:192.0.2.100/2947
```

```
        dst inside:192.168.60.115/80 by access-group "tACL-Policy"
  Jun 21 2009 00:15:13: %ASA-4-106023: Deny tcp src
outside:192.0.2.88/2949
        dst inside:192.168.60.38/443 by access-group "tACL-Policy"
  Jun 21 2009 00:15:13: %ASA-4-106023: Deny tcp src
outside:192.0.2.175/2950
        dst inside:192.168.60.250/443 by access-group "tACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *tACL-Policy* show **SSH** packets for **TCP port 22**, **HTTP** packets for **TCP port 80**, and **HTTPS** packets for **TCP port 443** sent to the address block assigned to the 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

Revision History

Revision 1.0	2009-July-27	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
- Securing Tool Command Language on Cisco IOS
- Cisco Firewall Products - Home Page on Cisco.com
- Common Vulnerabilities and Exposures (CVE)
