

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in the Cisco ACE Application Control Engine Module and Cisco ACE 4710 Application Control Engine

<http://www.cisco.com/warp/public/707/cisco-amb-20090225-ace.shtml>

Revision 1.1

Last Updated 2009 February 25 1900 UTC (GMT)

For Public Release 2009 February 25 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 *Multiple Vulnerabilities in the Cisco ACE Application Control Engine Module and Cisco ACE 4710 Application Control Engine* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

There are multiple vulnerabilities in Cisco ACE Application Control Engine Module and Appliance. The following subsections summarize three of these vulnerabilities that have a network mitigation:

Crafted Secure Shell (SSH) Packet 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. 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-2009-0623.

Crafted Simple Network Management Protocol Version 1 (SNMPv1) Packet 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. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through SNMP packets using UDP port 161. An attacker could exploit this vulnerability using spoofed packets.

This vulnerability has been assigned CVE identifier CVE-2009-0624.

Crafted SNMPv3 Packet 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. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through SNMP packets using UDP port 161. An attacker could exploit this vulnerability using spoofed packets.

This vulnerability has been assigned CVE identifier CVE-2009-0625.

Vulnerability Overview

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-20090225-ace.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 the following methods:

- Infrastructure access control lists (iACLs)
- Flexible Packet Matching (FPM)
- Unicast Reverse Path Forwarding (Unicast RPF)
- IP source guard (IPSG)

These protection mechanisms filter and drop, as well as verify the source IP address of, packets that are attempting to exploit these vulnerabilities.

The proper deployment and configuration of Unicast RPF provides an effective means of protection

against attacks that use packets with spoofed source IP addresses. Unicast RPF should be deployed as close to all traffic sources as possible.

The proper deployment and configuration of IPSG provides an effective means of protection against spoofing attacks at the access layer.

Because the potential exists that a trusted networking client could become affected by a worm that does not use packets with spoofed source addresses, Unicast RPF and IPSG do not provide complete protection against these vulnerabilities.

Effective means of 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 the following:

- Transit ACLs
- Application layer protocol inspection
- Unicast RPF

These protection mechanisms filter and drop, as well as verify the source IP address of, packets that are attempting to exploit these vulnerabilities.

Effective use of Cisco Intrusion Prevention System (IPS) event actions provides visibility into and protection against attacks that attempt to exploit the **Crafted SSH Packet Vulnerability** and the **Crafted SNMPv3 Packet Vulnerability**.

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can also provide visibility through incidents, queries, and event reporting.

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.

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 Intrusion Prevention System](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)

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

The iACL policy denies unauthorized SSH packets on TCP port 22 and SNMP packets on UDP port 161 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 22
    permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq snmp

!
!-- 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 22
deny udp any 192.168.60.0 0.0.0.255 eq snmp

!
!-- 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 unreachable**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable interval-in-ms**.

Mitigation: Flexible Packet Matching

The **crafted SNMPv1 packet** and **crafted SNMPv3 packet** vulnerabilities can be mitigated by Flexible Packet Matching (FPM). FPM was introduced in Cisco IOS Software Release[®] 12.4(4)T with the capability to deny specific packets based on content that is in the first 256 bytes of the packet. FPM was updated in release 12.4(15)T and can now search for patterns up to 256 bytes long anywhere in a packet. The [Flexible Packet Matching Deployment Guide](#) contains further information about FPM. In the case of the SNMP vulnerabilities covered in this Applied Mitigation Bulletin, FPM can be an effective means to block unwanted activity that is directed at the vulnerable device. For these vulnerabilities, FPM provides a way to differentiate among the different versions of SNMP messages and allows SNMPv2 traffic while denying SNMPv1 and SNMPv3 traffic. This capability is beyond that provided by a normal access list, which will drop all packets sent to UDP port 161 regardless of SNMP version.

In the following example, FPM will classify the SNMP traffic according to the version using two class maps: SNMPv1 and SNMPv3. The FPM policy is applied in the ingress direction and will block SNMPv1 and SNMPv3 packets. The capability to use field names in the match statement requires the use of Protocol Header Definition Files, which are available for download by registered users at <http://www.cisco.com/cgi-bin/tablebuild.pl/fpm>.

```
!
!-- Load Protocol Header Definition Files (PHDFs) for protocols IP and UDP.
!-- The PHDFs contain the definitions for the fields that will be used
!-- in this example.
!

load protocol flash:ip.phdf
load protocol flash:udp.phdf

!
!-- Class map to match on IP/UDP packets
!

class-map type stack match-all IP-UDP
  description * Match on UDP packets *
  match field IP protocol eq 17 next UDP

!
!-- Class map to match on SNMPv1 packets
!
```

```

class-map type access-control match-all SNMPv1
description * Match on SNMPv1 packets *
match field UDP dest-port eq 161
match start UDP payload-start offset 4 size 1 eq 0

!
!-- Class map to match on SNMPv3 packets
!

class-map type access-control match-all SNMPv3
description * Match on SNMPv3 packets *
match field UDP dest-port eq 161
match start UDP payload-start offset 4 size 1 eq 3

!
!-- Policy map that will classify SNMP versions.
!-- SNMPv1 and SNMPv3 will then be dropped and logged.
!

policy-map type access-control FPM-UDP-Policy
description * Drop and log SNMP v1 and v3 packets *
class SNMPv1
drop
log
class SNMPv3
drop
log

!
!-- With the Hierarchical Queuing Framework (HQF),
!-- the parent FPM policy "FPM-Policy" uses a
!-- child policy "FPM-UDP-Policy"
!-- for further classification.
!

policy-map type access-control FPM-Policy
description * Match on UDP *
class IP-UDP
service-policy FPM-UDP-Policy

!
!-- Apply FPM-Policy in the ingress direction
!

interface GigabitEthernet 0/0
service-policy type access-control input FPM-Policy

```

Mitigation: Spoofing Protection

Unicast Reverse Path Forwarding

All vulnerabilities that are described in this document can be exploited by spoofed IP packets. Administrators can deploy and configure Unicast Reverse Path Forwarding (Unicast RPF) as a protection mechanism against spoofing.

Unicast RPF is configured at the interface level and can detect and drop packets that lack a verifiable source IP address. Administrators should not rely on Unicast RPF to provide complete spoofing

protection because spoofed packets may enter the network through a Unicast RPF-enabled interface if an appropriate return route to the source IP address exists. Administrators are advised to take care to ensure that the appropriate Unicast RPF mode (loose or strict) is configured during the deployment of this feature because it can drop legitimate traffic that is transiting the network. In an enterprise environment, Unicast RPF might be enabled at the Internet edge and the internal access layer on the user-supporting Layer 3 interfaces.

Additional information is in the [Unicast Reverse Path Forwarding Loose Mode Feature Guide](#).

For additional information about the configuration and use of Unicast RPF, reference the [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence white paper.

IP Source Guard

IP source guard (IPSG) is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering packets based on the DHCP snooping binding database and manually configured IP source bindings. Administrators can use IPSG to prevent attacks from an attacker who attempts to spoof packets by forging the source IP address and/or the MAC address. When properly deployed and configured, IPSG coupled with strict mode Unicast RPF provides the most effective means of spoofing protection for the vulnerabilities that are described in this document.

Additional information about the deployment and configuration of IPSG is in [Configuring DHCP Features and IP Source Guard](#).

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 SSH packets on TCP port 22 and SNMP packets on UDP port 161 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 these vulnerabilities. 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 22
 20 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq snmp
 30 deny tcp any 192.168.60.0 0.0.0.255 eq 22 (121 matches)
 40 deny udp any 192.168.60.0 0.0.0.255 eq snmp (31 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:

- **121 SSH packets on TCP port 22** for ACE line 30
- **31 SNMP packets on UDP port 161** for ACE line 40

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.

Identification: Flexible Packet Matching

FPM can give detailed statistics of policy infractions.

```
Router#show policy-map type access-control interface GigabitEthernet0/0 input
GigabitEthernet0/0

Service-policy access-control input: FPM-Policy

Class-map: IP-UDP (match-all)
  769 packets, 86726 bytes
  5 minute offered rate 0 bps
  Match: field IP protocol eq 17 next UDP

Service-policy access-control : FPM-UDP-Policy

Class-map: SNMPv1 (match-all)
  10 packets, 860 bytes
  5 minute offered rate 0 bps
  Match: field UDP dest-port eq 161
  Match: start UDP payload-start offset 4 size 1 eq 0
drop

Class-map: SNMPv3 (match-all)
  19 packets, 2014 bytes
  5 minute offered rate 0 bps
  Match: field UDP dest-port eq 161
  Match: start UDP payload-start offset 4 size 1 eq 3
```

```

drop
log

Class-map: class-default (match-any)
  740 packets, 83852 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any

Class-map: class-default (match-any)
  5881 packets, 569093 bytes
  5 minute offered rate 9000 bps, drop rate 0 bps
  Match: any
Router#

```

In the preceding example, policy map *FPM-Policy* has dropped the following packets:

- **10 SNMPv1 packets on UDP port 161** for class map SNMPv1
- **19 SNMPv3 packets on UDP port 161** for class map SNMPv3

FPM log messages are similar to those produced by the access control list entry **log-input** keyword, except that FPM log messages do not contain a MAC address:

```

*Feb 20 11:27:23.231 CST: %SEC-6-IPACCESSLOGP: list SNMPv1 denied udp 192.168.2
(GigabitEthernet0/0 ) -> 192.168.128.2(161), 8 packets
*Feb 20 11:30:23.231 CST: %SEC-6-IPACCESSLOGP: list SNMPv3 denied udp 192.168.2
(GigabitEthernet0/0 ) -> 192.168.128.2(161), 72 packets

```

In the preceding example, the logged messages show potentially spoofed **SNMP** packets for **UDP port 161** that were blocked.

Identification: Spoofing Protection Using Unicast Reverse Path Forwarding

With Unicast RPF properly deployed and configured throughout the network infrastructure, administrators can use the **show cef interface type slot/port internal**, **show ip interface**, **show cef drop**, and **show ip traffic** commands to identify the number of packets that Unicast RPF has dropped.

Note: The **show command | begin regex** and **show command | include regex** command modifiers are used in the following examples to minimize the amount of output that administrators will need to parse to view the desired information. Additional information about command modifiers is in the [show command](#) sections of the Cisco IOS Configuration Fundamentals Command Reference.

```

router#show cef interface GigabitEthernet 0/0 internal | include drop
--          CLI Output Truncated          --
  ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0
router#

```

Note: **show cef interface type slot/port internal** is a hidden command that must be fully entered at the command-line interface. Command completion is not available for it.

```

router#show ip interface GigabitEthernet 0/0 | begin verify
--          CLI Output Truncated          --
IP verify source reachable-via RX, allow default, allow self-ping
11 verification drops
0 suppressed verification drops

```

```

router#

router#show cef drop
CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj  ChkSum_Err
RP      27           0           0           178      0       0
router#

router#show ip traffic

IP statistics:
Rcvd: 68051015 total, 2397325 local destination
      43999 format errors, 0 checksum errors, 33 bad hop count
      2 unknown protocol, 929 not a gateway
      21 security failures, 190123 bad options, 542768 with options
Opts: 352227 end, 452 nop, 36 basic security, 1 loose source route
      45 timestamp, 59 extended security, 41 record route
      53 stream ID, 3 strict source route, 40 alert, 45 cipso, 0 ump
      361634 other
Frgs: 0 reassembled, 10008 timeouts, 56866 couldn't reassemble
      0 fragmented, 0 fragments, 0 couldn't fragment
Bcast: 64666 received, 0 sent
Mcast: 1589885 received, 2405454 sent
Sent: 3001564 generated, 65359134 forwarded
Drop: 4256 encapsulation failed, 0 unresolved, 0 no adjacency
      178 no route, 178 unicast RPF, 0 forced drop
      0 options denied
Drop: 0 packets with source IP address zero
Drop: 0 packets with internal loop back IP address
      --      CLI Output Truncated      --
router#

```

In the preceding **show cef drop** and **show ip traffic** examples, Unicast RPF has dropped **178 IP packets** received globally on all interfaces with Unicast RPF configured because of the inability to verify the source address of the IP packets within the Forwarding Information Base of Cisco Express Forwarding.

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 (107204567 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .392 .234 .094 .066 .014 .038 .015 .002 .000 .007 .001 .000 .000 .001

   512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .000 .037 .019 .070 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes

```

```

27 active, 65509 inactive, 10686074 added
376190258 aged polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 533256 bytes
27 active, 16357 inactive, 10686074 added, 10686074 added to flow
0 alloc failures, 2161 force free
1 chunk, 6 chunks 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	10405	0.0	9	43	0.0	3.8	24.4
TCP-FTP	7990	0.0	2	52	0.0	1.0	48.7
TCP-FTPD	2999	0.0	460	600	0.3	0.6	46.7
TCP-WWW	176960	0.0	37	733	1.5	26.5	16.8
TCP-SMTP	5067	0.0	2	68	0.0	25.2	42.5
TCP-X	2853	0.0	1	43	0.0	0.0	50.6
TCP-BGP	2771	0.0	1	43	0.0	0.0	50.0
TCP-NNTP	2771	0.0	1	43	0.0	0.0	49.8
TCP-Frag	43	0.0	5	1204	0.0	0.7	60.1
TCP-other	7666029	1.7	8	194	14.3	1.2	26.7
UDP-DNS	185620	0.0	4	66	0.1	19.0	51.7
UDP-NTP	246315	0.0	1	76	0.0	5.1	58.5
UDP-TFTP	4	0.0	1	28	0.0	0.0	60.3
UDP-Frag	123	0.0	2074	1469	0.0	112.5	6.0
UDP-other	983056	0.2	30	125	7.0	20.6	52.1
ICMP	894686	0.2	2	75	0.4	3.8	59.9
IGMP	154777	0.0	2	39	0.0	58.8	42.3
IPINIP	4	0.0	16	137	0.0	84.8	26.5
IPv6INIP	5	0.0	12	143	0.0	69.7	31.8
GRE	466	0.0	1	20	0.0	0.2	60.4
IP-other	343104	0.0	10	95	0.7	91.2	16.9
Total:	10686048	2.4	10	209	24.9	7.8	32.8

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.208.64	Gi0/0	192.168.78.35	06	0D3D	077B	10
Gi0/0	192.168.208.127	Gi0/0	192.168.104.132	06	D8B0	1A29	6
Gi0/0	192.168.208.64	Gi0/0	192.168.108.24	06	DE61	0015	2
Gi0/0	192.168.60.63	Gi0/0	192.168.60.30	06	0016	12BD	3197
Gi0/0	192.168.60.127	Gi0/0	192.168.60.1	06	0016	086D	74
Gi0/0	192.168.60.127	Gi0/0	192.168.60.57	06	0016	086D	127
Gi0/0	192.168.208.127	Gi0/0	182.168.255.40	06	D1A9	0050	6
Gi0/0	192.168.208.111	Null	255.255.255.255	11	1375	2FBF	5
Gi0/0	192.168.208.127	Gi0/0	182.168.255.40	06	E8CA	0050	2
Gi0/0	192.168.208.84	Gi0/0	182.168.104.132	06	EAAB	1A29	2
Gi0/0	192.168.60.63	Gi0/1	192.168.60.2	11	8015	00A1	6
Gi0/0	192.168.60.63	Gi0/1	192.168.60.20	11	8015	00A1	144
Gi0/0	192.168.208.111	Null	255.255.255.255	11	DDA2	0035	1
Gi0/0	192.168.208.111	Null	255.255.255.255	11	CE92	0202	2

```
router#
```

In the preceding example, there are multiple flows for **SSH** packets on **TCP** port **22** (hex value **0016**) and **SNMP** packets on **UDP** port **161** (hex value **00A1**).

This traffic is sourced from and sent to addresses within the 192.168.60.0/24 address block, which is used for infrastructure devices. The packets in these flows may be spoofed and may indicate an attempt to exploit these vulnerabilities. Administrators are advised to compare these flows to baseline utilization for SSH packets on TCP port 22 and SNMP packets on UDP port 161 and also investigate the flows to

determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for SNMP packets on UDP port 161 (hex value 00A1), the command **show ip cache flow | include SrcIf|_11_.*00A1** will display the related UDP NetFlow records as shown here:

UDP Flows

```
router#show ip cache flow | include SrcIf|_11_.*00A1
SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pkts
Gi0/0     192.168.208.63 Gi0/1      192.168.60.2  11 8015 00A1   6
Gi0/0     192.168.208.63 Gi0/1      192.168.60.20 11 8015 00A1 144
router#
```

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

TCP Flows

```
router#show ip cache flow | include SrcIf|_06_.*0016
SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pkts
Gi0/0     192.168.208.63 Gi0/1      10.89.17.224  06 0016 12BD 3197
Gi0/0     192.168.208.127 Gi0/1      10.89.17.224  06 0016 086D   74
router#
```

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Application Layer Protocol Inspection

Application layer protocol inspection is available beginning in software release 7.2(1) for the Cisco ASA 5500 Series Adaptive Security Appliance and the Cisco PIX 500 Series Security Appliance and in software release 4.0(1) for the Firewall Services Module. This advanced security feature performs deep packet inspection of traffic that transits the firewall. Administrators may construct an inspection policy for applications that require special handling through the configuration of inspect class maps and inspect policy maps, which are applied via a global or interface service policy.

Additional information about application layer protocol inspection is in the [Applying Application Layer Protocol Inspection](#) section of the [Cisco Security Appliance Command Line Configuration Guide](#).



Caution: Application layer protocol inspection will decrease firewall performance. Administrators are advised to test performance impact in a lab environment before this feature is deployed in production environments.

SNMP Application Inspection

Using the SNMP application inspection engine on the Cisco ASA 5500 Series Adaptive Security Appliances, the Cisco PIX 500 Series Security Appliances, and the Firewall Services Modules, administrators can configure a policy that prevents SNMPv1 and SNMPv3 messages while allowing SNMPv2 messages to transit the firewall. The following SNMP application inspection uses the Modular Policy Framework (MPF) to create a policy for inspection of traffic on UDP port 161. The SNMP

inspection policy will drop SNMPv1 and SNMPv3 connections

```
!  
!-- Configure an SNMP map to deny SNMPv1 and SNMPv3 packets  
!  
snmp-map deny_SNMPv1_SNMPv3  
  deny version 1  
  deny version 3  
  
!  
!-- Add the above configured SNMP map to the default policy  
!-- "global_policy" and default class "inspection_default"  
!-- and use it to inspect SNMP traffic that transits the firewall  
!  
  
policy-map global_policy  
  class inspection_default  
    inspect snmp deny_SNMPv1_SNMPv3  
  
!  
!-- By default, the policy "global_policy" is applied globally,  
!-- which results in the inspection of traffic that enters the  
!-- firewall from all interfaces  
!  
  
service-policy global_policy global
```

Additional information about SNMP application inspection and the Modular Policy Framework is in the [SNMP Inspection](#) section of the Cisco Security Appliance Command Line Configuration Guide.

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 SSH packets on TCP port 22 and SNMP packets on UDP port 161 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
access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0 255

!
!-- 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 ssh
access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq snm

!
!-- 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

```

Mitigation: Spoofing Protection Using Unicast Reverse Path Forwarding

All vulnerabilities that are described in this document can be exploited by spoofed IP packets. Administrators can deploy and configure Unicast Reverse Path Forwarding (Unicast RPF) as a protection mechanism against spoofing.

Unicast RPF is configured at the interface level and can detect and drop packets that lack a verifiable source IP address. Administrators should not rely on Unicast RPF to provide complete spoofing protection because spoofed packets may enter the network through a Unicast RPF-enabled interface if an appropriate return route to the source IP address exists. In an enterprise environment, Unicast RPF might be enabled at the Internet edge and at the internal access layer on the user-supporting Layer 3 interfaces.

For additional information about the configuration and use of Unicast RPF, reference the Cisco Security Appliance Command Reference for [ip verify reverse-path](#) and the [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence white paper.

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 and SNMP packets on UDP port 161 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; 5 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1 192.168.6
access-list tACL-Policy line 2 extended permit udp host 192.168.100.1 192.168.6
access-list tACL-Policy line 3 extended deny tcp any 192.168.60.0 255.255.255.0

```

```
access-list tACL-Policy line 4 extended deny udp any 192.168.60.0 255.255.255.0
access-list tACL-Policy line 5 extended deny ip any any (hitcnt=0)
firewall#
```

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

- **410 SSH** packets on **TCP port 22** for ACE line 3
- **218 SNMP** packets on **UDP port 161** 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 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
Feb 21 2009 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.100/2947
dst inside:192.168.60.115/161 by access-group "tACL-Policy"
Feb 21 2009 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.88/2949
dst inside:192.168.60.38/161 by access-group "tACL-Policy"
Feb 21 2009 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.175/2950
dst inside:192.168.60.250/161 by access-group "tACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *tACL-Policy* show potentially spoofed **SNMP** packets for **UDP port 161** sent to the address block assigned to the infrastructure 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.

Identification: Application Layer Protocol Inspection

Firewall syslog message *416001* will be generated when an SNMP packet is dropped. The syslog

message will identify the SNMP version of the dropped packet. Additional information about this syslog message is in [Cisco Security Appliance System Log Message - 416001](#).

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 attempts to exploit these vulnerabilities. Administrators can use different regular expressions with the **grep** keyword to search for specific data in the logged messages

SNMP Application Inspection

```
firewall# show logging | grep 416001
Feb 18 2009 14:39:04: %ASA-4-416001: Dropped UDP SNMP packet
from outside:192.168.208.63/32790 to inside:192.168.210.13/161;
version (1) is not allowed thru the firewall
Feb 18 2009 14:39:05: %ASA-4-416001: Dropped UDP SNMP packet
from outside:192.168.208.63/32790 to inside:192.168.210.13/161;
version (3) is not allowed thru the firewall
```

With SNMP inspection enabled, the **show service-policy** command will identify the number of SNMP packets inspected and dropped by this feature. The following example shows output for **show service-policy**:

```
firewall# show service-policy | include snmp
Inspect: snmp deny SNMPv1 SNMPv3, packet 3188266, drop 210, reset-drop 0
firewall#
```

In the preceding example, **3,188,266 SNMP packets** have been inspected and **210 SNMP packets** have been dropped.

Identification: Spoofing Protection Using Unicast Reverse Path Forwarding

Firewall syslog message *106021* will be generated for packets denied by Unicast RPF. Additional information about this syslog message is in [Cisco Security Appliance System Log Message - 106021](#).

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 106021
Feb 21 2007 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
      192.168.60.1 to 192.168.60.100 on interface outside
Feb 21 2007 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
      192.168.60.1 to 192.168.60.100 on interface outside
Feb 21 2007 00:15:13: %ASA-1-106021: Deny TCP reverse path check from
      192.168.60.1 to 192.168.60.100 on interface outside
firewall#
```

The **show asp drop** command can also identify the number of packets that the Unicast RPF feature has dropped, as shown in the following example:

```
firewall#show asp drop frame rpf-violated
Reverse-path verify failed                2011
firewall#
```

In the preceding example, Unicast RPF has dropped **2,011 IP packets** received on interfaces with Unicast RPF configured. Absence of output indicates that the Unicast RPF feature on the firewall has not dropped packets.

For additional information about debugging accelerated security path dropped packets or connections, reference the Cisco Security Appliance Command Reference for [show asp drop](#).

Cisco Intrusion Prevention System

Mitigation: Cisco IPS Signature Event Actions

Administrators can use Cisco Intrusion Prevention System (IPS) appliances and services modules to provide threat detection and help prevent attempts to exploit some of the vulnerabilities that are described in this document. These vulnerabilities may be detected by the following signatures:

- 15634/0 - Cisco ACE Crafted SSH Packet Vulnerability
- 15653/0 - Crafted SNMPv3 packet may crash ACE appliance

15634/0 - Cisco ACE Crafted SSH Packet Vulnerability

Beginning with signature update S384 for sensors running Cisco IPS version 6.x or 5.x, these vulnerabilities can be detected by signature 15634/0 (Signature Name: Cisco ACE Crafted SSH Packet Vulnerability). Signature 15634/0 is enabled by default, triggers a *High* severity event, has a signature fidelity rating (SFR) of 85, and is configured with a default event action of **produce-alert**.

Signature 15634/0 fires when a single packet sent using TCP port 22 is detected. Firing of this signature may indicate a potential exploit of the **Crafted SSH Packet Vulnerability**.

15653/0 - Crafted SNMPv3 packet may crash ACE appliance

Beginning with signature update S384 for sensors running Cisco IPS version 6.x or 5.x, these vulnerabilities can be detected by signature 15653/0 (Signature Name: Crafted SNMPv3 packet may crash ACE appliance). Signature 15653/0 is enabled by default, triggers a *Medium* severity event, has a signature fidelity rating (SFR) of 75, and is configured with a default event action of **produce-alert**.

Signature 15653/0 fires when a single packet sent using UDP port 161 is detected. Firing of this signature may indicate a potential exploit of the **Crafted SNMPv3 Packet Vulnerability**.

Administrators can configure Cisco IPS sensors to perform an event action when an attack is detected. The configured event action performs preventive or deterrent controls to help protect against an attack that is attempting to exploit the vulnerabilities that are described in this document.

Exploits that use spoofed IP addresses may cause a configured event action to inadvertently deny traffic from trusted sources.

Cisco IPS sensors are most effective when deployed in inline protection mode combined with the use of an event action. Automatic Threat Prevention for Cisco IPS 6.x sensors that are deployed in inline protection mode provides threat prevention against an attack that is attempting to exploit the vulnerabilities that are described in this document. Threat prevention is achieved through a default override that performs an event action for triggered signatures with a *riskRatingValue* greater than 90.

Cisco IPS 5.x sensors that are deployed in inline protection mode require an event action configured on a per-signature basis. Alternatively, administrators can configure an override that can perform an event action for any signatures that are triggered and are calculated as a high-risk threat. Using an event action on sensors deployed in inline protection mode provides the most effective exploit prevention.

For additional information about the risk rating and threat rating calculation, reference [Risk Rating and Threat Rating: Simplify IPS Policy Management](#).

Identification: IPS Signature Events

Signature: 15634/0 - Cisco ACE Crafted SSH Packet Vulnerability

```
IPS# show events alert
evIdsAlert: eventId=1229636522722245403 severity=high vendor=Cisco
originator:
  hostId: IPS
  appName: sensorApp
  appInstanceId: 419
time: 2009/02/25 15:10:54 2009/02/25 09:10:54 CST
signature: description=Cisco ACE Crafted SSH Packet Vulnerability id=15634 cr
  subsigId: 0
  sigDetails: Cisco ACE Crafted SSH Packet Vulnerability
  marsCategory: Penetrate/All
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 192.168.208.63
    port: 33463
  target:
    addr: locality=OUT 192.168.210.13
    port: 22
  os: idSource=unknown relevance=unknown type=unknown
actions:
  denyPacketRequestedNotPerformed: true
  denyFlowRequestedNotPerformed: true
```

```
context:
  fromAttacker:

!
!-- Packet details removed
!

triggerPacket:

!
!-- Packet details removed
!

riskRatingValue: targetValueRating=medium watchlist=25 95
threatRatingValue: 95
interface: ge0_3
protocol: tcp
```

15653/0 - Crafted SNMPv3 packet may crash ACE appliance

```
IPS# show events alert
evIdsAlert: eventId=1229636522722245906 vendor=Cisco severity=medium
originator:
  hostId: IPS
  appName: sensorApp
  appInstanceId: 419
time: Feb 25, 2009 17:49:39 UTC offset=-360 timeZone=CST
signature: description=Crafted SNMPv3 packet may crash ACE appliance id=15
  subSigId: 0
  sigDetails: Crafted SNMPv3 packet may crash ACE appliance
  marsCategory: Penetrate/All
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: 192.168.208.63 locality=OUT
    port: 32802
  target:
    addr: 192.168.210.13 locality=OUT
    port: 161
    os: idSource=unknown type=unknown relevance=unknown
triggerPacket:

!
!-- Packet details removed
!

riskRatingValue: 66 targetValueRating=medium watchlist=25
threatRatingValue: 66
interface: ge0_3
protocol: udp
```

Cisco Security Monitoring, Analysis, and Response System

Identification: Cisco Security Monitoring, Analysis, and Response System Incidents

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can

create incidents regarding events that are related to the vulnerabilities that are described in this document using IPS signature 15634/0 (Signature Name: Cisco ACE Crafted SSH Packet Vulnerability) and 15653/0 (Signature Name: Crafted SNMPv3 packet may crash ACE appliance). After the S384 dynamic signature update has been downloaded, using keyword **NR-15634/0** or **NR-15653/0** for IPS signatures 15634/0 or 15653/0 and a query type of **All Matching Events** on the Cisco Security MARS appliance will provide a report that lists the incidents created by the IPS signature.

Beginning with the 4.3.1 and 5.3.1 releases of Cisco Security MARS appliances, support for the Cisco IPS dynamic signature updates feature has been added. This feature downloads new signatures from Cisco.com or from a local web server, correctly processes and categorizes received events that match those signatures, and includes them in inspection rules and reports. These updates provide event normalization and event group mapping, and they also enable the MARS appliance to parse new signatures from the IPS devices.



Caution: If dynamic signature updates are not configured, events that match these new signatures appear as *unknown event type* in queries and reports. Because MARS will not include these events in inspection rules, incidents may not be created for potential threats or attacks that occur within the network.

By default, this feature is enabled but requires configuration. If it is not configured, the following Cisco Security MARS rule will be triggered:

System Rule: CS-MARS IPS Signature Update Failure

When this feature is enabled and configured, administrators can determine the current signature version downloaded by MARS by selecting **Help > About** and reviewing the *IPS Signature Version* value.

Additional information about dynamic signature updates and instructions for configuring dynamic signature updates are available for the Cisco Security MARS [4.3.1](#) and [5.3.1](#) releases.

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	2009- February-25	Include IPS Signature pack S384 and related MARS information.
Revision 1.0	2009- February-25	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](#)
- [Understanding Control Plane Protection](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Cisco ACE Application Control Engine Module Documentation](#)
- [Common Vulnerabilities and Exposures \(CVE\)](#)
- [Cisco 6.x Intrusion Prevention System](#)
- [Cisco IPS 6.x Signature Downloads](#) ([registered](#) customers only)
- [Cisco IPS Signature Search Page](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)

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](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)