

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of Multiple Vulnerabilities in the Cisco WLC and Cisco Lightweight APs

Document ID: 91288

<http://www.cisco.com/warp/public/707/cisco-amb-20070412-wlc.shtml>

## Revision 1.0

For Public Release 2007 April 12 1600 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 "Multiple Vulnerabilities in the Cisco Wireless LAN Controller and Cisco Lightweight Access Points" and documents additional mitigation techniques that can be deployed on Cisco devices within the network.

## Vulnerability Characteristics

The Cisco Wireless LAN Controller (WLC) and Lightweight Access Point (LWAP) contain multiple vulnerabilities that may result in a denial of service (DoS) condition or allow an attacker to take complete control of the affected device:

- **Default SNMP community strings.** The WLC uses the commonly known values of *public* and *private* for its read-only and read-write SNMP community strings. This vulnerability can be exploited remotely with a well-known credential and no user interaction is necessary. Exploitation may allow the attacker to take complete control of the affected device. This vulnerability is not covered by a CVE ID.
- **Malformed Ethernet traffic crash.** It is possible to cause one or more network processing units (NPUs) of an affected WLC to lock up by sending malformed wired traffic. This can result in a partial or complete inability to forward traffic. This is a local segment vulnerability; no further mitigations for this vulnerability will be mentioned in this document. This vulnerability is not covered by a CVE ID.
- **Multiple NPU lockup vulnerabilities.** It is possible to cause one or more NPUs of an affected WLC to lock up by sending wireless traffic with unexpected length or header values. This can result in a partial or complete inability to forward traffic. This is a local segment vulnerability; no further mitigations for this vulnerability will be mentioned in this document. This vulnerability is not covered by a CVE ID.

- **Hard-coded service password in LWAP.** Because a physical connection to the console port of the affected device is required to exploit this vulnerability, no further mitigations for this vulnerability will be mentioned in this document. This vulnerability is not covered by a CVE ID.
- **WLAN ACL does not persist through reboot.** The WLC contains a bug in its processing of WLAN access control lists (ACLs) that causes the WLAN ACL configuration to be saved with an invalid checksum. No further mitigations for this vulnerability will be mentioned in this document. This vulnerability is not covered by a CVE ID.

This document contains information to assist Cisco customers in identifying and mitigating attempts to exploit the multiple vulnerabilities in the Cisco WLC and Cisco LWAPs. Information about vulnerable, unaffected, and fixed software is available in the PSIRT security advisory:

<http://www.cisco.com/warp/customer/707/cisco-sa-20070412-wlc.shtml> .

## Mitigation Technique Overview

Cisco devices provide several countermeasures for the vulnerabilities in the Cisco WLC and Cisco LWAP. The most effective means of exploit prevention is provided by applying configuration changes directly to the affected devices as detailed in the PSIRT advisory.

Access control lists applied on Cisco IOS Software, PIX Security Appliances, Cisco ASA Adaptive Security Appliances, and Cisco Firewall Service Modules (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers can offer mitigation and provide defense in depth for the default SNMP community strings vulnerability. Unicast Reverse Path Forwarding (Unicast RPF) can also provide defense and limit the vectors through which the default SNMP community strings vulnerability can be exploited.

Detective controls can be performed using Cisco IOS NetFlow. The Cisco ASA Adaptive Security Appliance, Cisco PIX Security Appliance, and the FWSM for Cisco Catalyst 6500 Series switches and 7600 Series routers can also provide detective controls through syslog messages and counter values displayed in the output from **show** commands.

## Risk Management

Organizations should follow their standard risk mitigation process to determine the potential impact of these vulnerabilities. Documents that may be used to aid in the risk triage are available at [Risk Triage for Security Vulnerability Announcements](#) and [Risk Triage and Prototyping](#).

## 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. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround is the most appropriate for use in the intended network before it is deployed.

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

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

## Cisco IOS Routers

### Mitigation: Infrastructure Access Control Lists

In an effort to protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, infrastructure access control lists (iACL) should be deployed to perform policy enforcement of traffic sent to infrastructure equipment. The construction of an iACL is accomplished by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. iACLs deployed on Cisco IOS routers should be applied to all interfaces (where a Layer 3 IP address is configured) in the ingress direction for maximum protection of infrastructure devices.

In the following example, the address 192.0.2.2 belongs to the Wireless Control System (WCS), and the address 192.168.2.3 belongs to the WLC. The iACL policy permits SNMP packets (UDP port 161) from the WCS to the WLC and denies all other SNMP flows to this device.

Added access control entries (ACEs) should be implemented as part of an iACL policy that is used to filter traffic at network ingress points.

For more information on iACLs, refer to [Protecting Your Core: Infrastructure Protection Access Control Lists](#).

```
!-- Permit/deny additional Layer 3 and Layer 4 traffic sent to the
!-- infrastructure address space in accordance with existing security
!-- policies and configurations.

!-- Permit SNMP packets from known trusted host (WCS) to the WLC

access-list 101 permit udp host 192.0.2.2 gt 1023 host 192.168.2.3 eq snmp

!-- The following vulnerability-specific ACE
!-- aids in the identification of attacks.

access-list 101 deny udp any host 192.168.2.3 eq snmp

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

access-list 101 deny ip any 192.168.2.0 0.0.0.255

!-- Permit/deny all other Layer 3 or Layer 4 traffic in accordance with
!-- existing security policies and configurations.

!

!-- Apply access list to interface in the inbound direction.

interface FastEthernet0/0 ip
access-group 101 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. This could have the undesired effect of increasing CPU utilization because the filtering device needs to generate these ICMP unreachable messages. In IOS, ICMP unreachable generation is limited to one packet every 500 milliseconds. ICMP unreachable message generation can be disabled using the interface configuration command **no icmp unreachables**. ICMP unreachable rate limiting

can be changed from the default of one per 500 milliseconds using the global configuration command `ip icmp rate-limit unreachable interval-in-ms`.

## Mitigation: Anti-Spoof Protection Using Reverse Path Forwarding

The default SNMP community strings vulnerability described in this document can be exploited by spoofed packets. Protection mechanisms for anti-spoofing exist through the proper deployment and configuration of Unicast Reverse Path Forwarding (Unicast RPF). Unicast RPF is configured at the interface level and can detect and drop (discard) packets received on a Layer 3 interface if the packets lack a verifiable IP source address. Unicast RPF should not be relied on to provide 100 percent protection because spoofed packets may still enter the network through a Unicast RPF-enabled interface for which there is a suitable return route to the IP source address or the packet may be explicitly allowed by anti-spoofing access lists. Care must be taken to ensure that the appropriate Unicast RPF mode (loose or strict) is configured during the deployment of this feature. An incorrect deployment may drop legitimate traffic. Asymmetric traffic flows may be of concern when deploying this feature and Unicast RPF loose mode is a scalable option for traffic of this type. However, loose mode Unicast RPF does not provide effective threat mitigation for this vulnerability. Additional information about Unicast RPF is available at [Unicast Reverse Path Forwarding Loose Mode](#) and [Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider \(ISP\)](#).

iACLs coupled with anti-spoofing protection mechanisms via Unicast RPF provide an added layer of threat mitigation for this vulnerability. iACLs can also be used as a form of limited anti-spoofing protection by explicitly creating access control list entries (ACEs) that deny source addresses of the infrastructure IP address space.

There are Best Current Practices (BCPs) distributed through the Internet Engineering Task Force ([IETF](#)) that provide methods for limiting the risk and impact to the network and infrastructure from attacks that use spoofed source addresses. "Ingress Filtering for Multihomed Networks" ([BCP84](#)) and "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" ([BCP38](#)) are the BCPs that provide information and suggestions regarding how to mitigate spoofing attacks.

## Identification: Infrastructure Access Control Lists

With an iACL, once the access list has been applied to an interface in the ingress direction, the `show access-list` command can be used to identify the number of SNMP packets on UDP port 161 that are being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. Example output for `show access-list 101` follows. In this example, there were **7 packets** destined for the WLC on UDP port 161 dropped by access list 101. This access list has been applied in the inbound direction on interface FastEthernet0/0.

```
router#show access-list 101
Extended IP access list 101
 10 permit udp host 192.0.2.2 gt 1023 host 192.168.2.3 eq snmp
 20 deny udp any host 192.168.2.3 eq snmp (7 matches)
 30 deny ip any 192.0.2.0 0.0.0.255
router#
```

## Identification: Access List Logging

The `log` or `log-input` 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.

Note that ACL logging can be very CPU intensive and must be used with extreme caution. The CPU impact from ACL logging is driven by two factors: process switching as a result of packets matching log enabled ACEs and log generation and transmission. The CPU impact from ACL logging can be addressed in hardware

on the Catalyst 6500 Series switches and Cisco 7600 Series routers with Supervisor 720 and Supervisor 32 using [Optimized ACL Logging](#) or [Hardware Rate Limiting](#). The **ip access-list logging interval interval-in-ms** command can limit the effects of ACL logging-induced process switching. The **logging rate-limit rate-per-second except loglevel** command limits the impact of log generation and transmission.

The configuration below illustrates logging best practices in addition to the **ip access-list logging interval** and **logging rate-limit** commands. The **ip access-list logging interval 60000** command limits log-induced software processing to one packet per source per 60 seconds (60,000 ms). The **logging rate-limit 20 except 4** command shown below limits log generation and transmission to 20 messages per second except for log level 4 (warning) through level 0 (emergencies).

```
! -- Configure timestamps for syslog messages with date and time in milliseconds.
service timestamps log datetime msec

!-- Enable logging
logging on

!-- Disable CPU-intensive console logging and monitor logging.
no logging console
no logging monitor

!-- Configure logging level, log buffer size, and rate limiting.
logging buffered informational
logging buffered 16386
logging rate-limit 20 except 4

!-- Configure logging host.
logging 192.0.2.3

!-- The following is a vulnerability-specific ACE.
ip access-list logging interval 60000

!-- Configure access list with logging enabled for vulnerability-specific ACE.
!-- This is the same access list as shown in the mitigation section above.
access-list 101 permit udp host 192.0.2.2 gt 1023 host 192.168.2.3 eq snmp

!-- Vulnerability specific ACE with the "log" keyword appended.
access-list 101 deny udp any host 192.168.2.3 eq snmp log

!-- Explicit deny ACE for traffic sent to addresses configured
!-- within the infrastructure address space.
access-list 101 deny ip any 192.0.2.0 0.0.0.255

!-- Permit/deny all other Layer 3 or Layer 4 traffic in accordance with
!--existing security policies and configurations.
!

!-- Apply access list to interface in the inbound direction.
interface FastEthernet0/0 ip
access-group 101 in
```

## Identification: Anti-Spoof Protection Using Unicast Reverse Path Forwarding

With Unicast RPF properly deployed and configured throughout the network infrastructure, the **show ip interface**, **show cef drop**, **show cef interfacetype slot / port**, and **show ip traffic** commands can be used to identify the number of packets that Unicast RPF has dropped (discarded).

```
router#show ip interface gig 0/1
GigabitEthernet0/1 is up, line protocol is up
Internet address is 192.168.206.20/24
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.10 224.0.0.5 224.0.0.6
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is enabled
IP CEF switching is enabled
IP Selective flow switching turbo vector
IP Flow CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, Flow cache, CEF, Subint Flow
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
IP verify source reachable-via RX, allow default, allow self-ping
354 verification drops
0 suppressed verification drops
```

```
router#show cef drop
CEF Drop Statistics
Slot Encap_fail Unresolved Unsupported No_route No_adj ChkSum_Err
RP 4262 0 509 354 0 0
```

```
router#show cef interface gig 0/1
GigabitEthernet0/1 is up (if_number 3)
Corresponding hwidb fast_if_number 3
Corresponding hwidb firstsw->if_number 3
Internet address is 192.168.206.20/24
ICMP redirects are always sent Per packet load-sharing is disabled
IP unicast RPF check is enabled
Inbound access list is not set Outbound access list is not set
Hardware idb is GigabitEthernet0/1
Fast switching type 1, interface type 27
IP CEF switching enabled
IP Selective flow switching turbo vector
```

```
IP Flow CEF switching turbo vector
Input fast flags 0x0, Input fast flags2 0x8, Output fast flags 0x0,
  Output fast flags2 0x1
ifindex 3(3)
Slot 0 Slot unit 1 Unit 1 VC -1
Transmit limit accumulator 0x0 (0x0)
IP MTU 1500
```

```
router#show ip traffic
```

```
IP statistics:
```

```
Rcvd: 97600951 total, 4483904 local destination
  43999 format errors, 0 checksum errors, 553 bad hop count
  2 unknown protocol, 929 not a gateway
  21 security failures, 190123 bad options, 542769 with options
Opts: 352227 end, 453 nop, 36 basic security, 2 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
Frag: 0 reassembled, 10008 timeouts, 56866 couldn't reassemble
  0 fragmented, 0 fragments, 0 couldn't fragment
Bcast: 132235 received, 0 sent
Mcast: 3259182 received, 4924888 sent
Sent: 5859033 generated, 92776950 forwarded
Drop: 4262 encapsulation failed, 0 unresolved, 0 no adjacency
  354 no route, 43502 unicast RPF, 509 forced drop
  0 options denied
Drop: 0 packets with source IP address zero
Drop: 0 packets with internal loop back IP address
```

Remainder of **show ip traffic** output has been truncated.

## Cisco IOS Switches

### Mitigation: Infrastructure Access Control Lists

In an effort to protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, infrastructure access control lists (iACLs) should be deployed to perform policy enforcement of traffic sent to infrastructure equipment. The construction of an iACL is accomplished by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. iACLs deployed on Cisco IOS switches should be applied to all interfaces (where a Layer 3 IP address is configured) in the ingress direction for maximum protection of infrastructure devices.

Layer 3 access lists may be deployed on a Cisco IOS switch VLAN interface. The following access list will permit SNMP traffic (UDP port 161) from the WCS (for example 192.0.2.2) to the WLC (for example 192.168.2.3) and filter all other SNMP traffic destined for the WLC.

Added access list entries should be implemented as part of an iACL that filters traffic on and to infrastructure devices.

For more information on infrastructure ACLs, refer to [Protecting Your Core: Infrastructure Protection Access Control Lists](#)

```
!-- Permit/deny additional Layer 3 and Layer 4 traffic sent to the
! -- infrastructure address space in accordance with existing security
! -- policies and configurations.
```

```
!-- Permit SNMP packets from known trusted host (WCS) to the WLC.
```

```

access-list 101 permit udp host 192.0.2.2 gt 1023 host 192.168.2.3 eq snmp

!-- The following vulnerability-specific ACE
!-- aids in the identification of attacks.

access-list 101 deny udp any host 192.168.2.3 eq snmp

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

access-list 101 deny ip any 192.168.2.0 0.0.0.255

!-- Permit/deny all other Layer 3 or Layer 4 traffic in accordance with
!-- existing security policies and configurations.

!

!-- Apply access list to interface in the inbound direction.

interface Vlan101
ip access-group 101 in

```

## Mitigation: Anti-Spoof Protection Using IP Source Guard

The default SNMP community strings vulnerability can be exploited by spoofed packets. A method of providing some protection against spoofed packets exists with IP source guard. IP source guard is a security feature that restricts IP traffic on non-routed Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and manually configured IP source bindings. IP source guard can be used to help prevent attacks from a malicious user who tries to spoof packets by forging the source IP address and/or the MAC address. When properly configured and deployed on a switch, IP source guard with strict mode Unicast RPF provides the most effective means of anti-spoofing protection for the default SNMP community strings vulnerability.

After IP source guard has been enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping. A port access control list (PACL) is applied to the interface. The PACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.

The IP source binding table has entries that are learned by DHCP snooping or manually configured. An entry in this table has an IP address, an associated MAC address, and an associated VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.

IP source guard is supported only on Layer 2 interfaces, including access and trunk ports. IP source guard can be configured for IP address filtering or with source IP and MAC address filtering.

Additional information about IP source guard is available at [Configuring DHCP Features and IP Source Guard](#).

## Identification: Infrastructure Access Control Lists

When a Layer 3 access list has been applied to a VLAN interface, the **show access-list** command can be used to identify the number of packets being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. Example output for **show access-list 101** follows. In this example, there were **4 packets** destined for the WLC on UDP port 161 and dropped by access list 101. The access list has been applied to VLAN interface 101 in the inbound direction.

```

Cat6509E#show access-list 101
Extended IP access list 101
 10 permit udp host 192.0.2.2 gt 1023 host 192.168.2.3 eq snmp

```

```

20 deny udp any host 192.168.2.3 eq snmp (4 matches)
30 deny ip any host 192.168.2.0 0.0.0.255

```

## Cisco IOS NetFlow

### Identification: Traffic Flow Identification Using NetFlow Records

Cisco IOS NetFlow can be configured on Cisco IOS routers and switches to aid in the identification of traffic flows that may be potential attempts to exploit the default SNMP community strings vulnerability. Packets should be investigated to determine whether they are attempts to exploit this vulnerability or legitimate traffic.

```

router#show ip cache flow
IP packet size distribution (2627001 total packets):
  1-32  64   96   128  160  192  224  256  288  320  352  384  416  448  480
    .907 .033 .043 .000 .014 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

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

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 419982 added
  10096949 aged polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 17416 bytes
  0 active, 1024 inactive, 74 added,
  74 added to flow
  0 alloc failures, 0 force free 1 chunk,
  1 chunk added
  last clearing of statistics never

```

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telnet	735	0.0	20	41	0.0	4.0	14.9
TCP-FTP	735	0.0	6	56	0.0	9.3	10.8
TCP-X	4	0.0	1	40	0.0	0.0	15.4
TCP-BGP	30458	0.0	1	44	0.0	0.0	15.5
TCP-other	8943	0.0	1	44	0.0	0.0	15.0
UDP-NTP	28496	0.0	1	77	0.0	0.0	15.5
UDP-other	265145	0.1	1	28	0.1	0.0	15.5
ICMP	85173	0.0	24	28	1.0	32.0	15.5
GRE	216	0.0	569	109	0.0	1798.6	1.8
IP-other	75	0.0	380	60	0.0	1756.7	2.6
Total:	419980	0.2	6	33	1.2	7.7	15.4

```

SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP      Pkts
-----
Gi0/0      192.0.2.2          Gi0/1      192.168.2.3       11 0B2A 00A1     187
Gi0/0      10.82.217.144     Gi0/1      192.168.128.21    06 12FF 0017      5
Gi0/0      192.168.212.32    Gi0/1      192.168.2.3       11 077B 00A1     140
Gi0/0      192.168.202.22    Gi0/1      192.168.138.23    2F 0000 0000     202
Gi0/0      192.168.7.144     Gi0/1      192.168.2.3       06 020F 0017      73
router#

```

In the preceding example, there are several flows of SNMP packets on UDP port 161 (hex value 00A1). This traffic is being sourced from addresses in the 192.168.x.x address block (which is untrusted), sourced from 192.0.2.2 (which is the WCS), and destined for IP address 192.168.2.3 (which is the WLC). These flows should be compared to baseline utilization for SNMP traffic and should also be investigated to determine whether the flows are sourced from trusted hosts and networks.

```

router#show ip cache flow
IP packet size distribution (127490425 total packets):
  1-32  64   96   128  160  192  224  256  288  320  352  384  416  448  480

```

```
.009 .620 .037 .007 .008 .008 .005 .012 .000 .001 .004 .001 .002 .002 .007
```

```
512 544 576 1024 1536 2048 2560 3072 3584 4096 4608  
.000 .001 .189 .012 .065 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 4456704 bytes
```

```
21 active, 65515 inactive, 64114757 added  
189393915 aged polls, 0 flow alloc failures  
Active flows timeout in 1 minutes  
Inactive flows timeout in 15 seconds
```

```
IP Sub Flow Cache, 402056 bytes
```

```
21 active, 16363 inactive, 3642269 added, 3642269 added to flow  
0 alloc failures, 0 force free  
1 chunk, 11 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	11403756	2.6	1	49	3.0	0.0	1.5
TCP-FTP	6777	0.0	8	53	0.0	6.0	7.7
TCP-FTPD	673	0.0	3294	889	0.5	53.4	0.5
TCP-WWW	164760	0.0	13	749	0.5	4.2	9.2
TCP-SMTP	12	0.0	1	47	0.0	0.0	10.5
TCP-X	731	0.0	1	40	0.0	0.0	1.4
TCP-BGP	13	0.0	1	46	0.0	0.0	10.3
TCP-NNTP	12	0.0	1	47	0.0	0.0	9.7
TCP-Frag	70399	0.0	1	688	0.0	0.0	22.7
TCP-other	49138086	11.4	2	264	23.9	0.0	1.4
UDP-DNS	908876	0.2	1	58	0.2	0.0	15.4
UDP-NTP	1145588	0.2	1	76	0.2	0.6	15.5
UDP-TFTP	10	0.0	2	57	0.0	6.6	18.6
UDP-other	1008015	0.2	1	164	0.4	0.3	16.7
ICMP	266155	0.0	8	47	0.5	13.3	21.1
IPv6INIP	15	0.0	1	1132	0.0	0.0	15.4
GRE	694	0.0	1	50	0.0	0.0	15.4
IP-other	2	0.0	2	20	0.0	0.1	15.7
Total:	64114574	14.9	1	252	29.6	0.1	2.2

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.160.4	Null	192.168.2.3	11	048B	00A1	81
Gi0/0	192.168.160.5	Null	192.168.2.3	11	032B	00A1	11
Gi0/0	10.21.121.14	Gi0/1	192.168.210.11	06	C879	01BB	30
Gi0/0	10.21.121.14	Gi0/1	192.168.210.11	06	C879	01BB	30
Gi0/0	192.0.2.2	Gi0/1	192.168.2.3	11	0731	00A1	123
Gi0/0	192.168.134.7	Gi0/1	192.168.160.7	11	0401	0035	17

```
router#
```

In the preceding example, there several flows of SNMP packets on UDP port 161 (hex value 00A1). This traffic has been determined to have originated from spoofed IP addresses and may indicate an attempt to exploit the vulnerability described in this document. The traffic associated with these flows is identified as spoofed because Unicast RPF has been enabled on the interfaces of this device and the destination interface value (DstIF) is **Null**. This traffic resulted in failure of the verification check for the source IP address within the packet because the 192.168.160.0/24 address block is reachable via GigabitEthernet0/1 based on the Cisco Express Forwarding (CEF) Forwarding Information Base (FIB) table. These packets were dropped (discarded) by the Unicast RPF feature and the flows should be investigated to determine the source of the spoofed traffic.

## Cisco ASA, PIX, and FWSM Firewalls

## Mitigation: Transit Access Control Lists

In an effort to protect the network from edge traffic that enters the network at ingress access points or traffic that transits the network, transit access control lists (tACLs) should be deployed to perform policy enforcement for this traffic. The construction of a tACL is accomplished 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.

These access control entries (ACEs) may be deployed on a Cisco ASA, PIX, or FWSM firewall as part of a firewall policy that will protect devices deployed behind it, including the WLC. The following access list permits SNMP traffic (UDP port 161) from a WCS (for example 192.0.2.2) to a WLC (for example 192.168.2.3) and filters all other SNMP traffic destined for the WLC.

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 service segments. Using this methodology will assist with the construction and deployment of tACLs.

Additional information about tACLs is available at [Transit Access Control Lists: Filtering at Your Edge](#).

```
!-- Permit/deny additional Layer 3 and Layer 4 traffic un/authorized to enter
!-- the network at ingress access points or traffic that has been un/authorized
!-- to transit the network in accordance with existing security policies
!-- and configurations. Deny all SNMP packets on port UDP/161 sent to any IP
!-- address configured within the address block of 192.0.2.0/24, which is
!-- the infrastructure address space, except from known trusted source networks
!-- (ex: management networks, security operations center, network operations
!-- center).

!-- Permit SNMP packets from known trusted host (WCS) to the WLC.

access-list outside extended permit udp host 192.0.2.2 gt 1023 host 192.168.2.3 eq snmp

!-- The following vulnerability-specific ACE aids
!-- in the identification of attacks.

access-list outside extended deny udp any host 192.168.2.3 eq snmp

!-- Explicit default deny for unauthorized traffic entering the network
!-- at ingress access points or unauthorized transit traffic sent to addresses
!-- configured within the infrastructure address space.

access-list outside extended deny ip any 192.168.2.0 0.0.0.255

!-- Permit/deny all other IP traffic in accordance
!-- with existing security policies and configuration.

!

!-- Apply access list to interface in the inbound direction.

access-group outside in interface outside
```

## Identification: Transit Access Control Lists

With a tACL, once the access list has been applied to an interface in the ingress direction, the **show access-list** command can be used to identify the number of SNMP packets on UDP port 161 that are being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. Example output for **show access-list outside** follows:

```

firewall# show access-list outside
access-list outside; 3 elements
access-list outside line 1 extended permit udp host 192.0.2.2 gt 1023 host
192.168.2.3 eq snmp (hitcnt=0) 0xd171b2e8
access-list outside line 2 extended deny udp any host 192.168.2.3 eq snmp
(hitcnt=5) 0x903d520a
access-list outside line 3 extended deny udp any 192.168.2.0 0.0.0.255
(hitcnt=0) 0x1a062f33
firewall#

```

In the preceding example, **access-list outside** has dropped **5 UDP port 161 packets** received from a untrusted host or network. This tACL is applied to interface *outside* in the ingress direction. 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 protocol for the denied packet.

## Identification: Firewall Syslog Messages

Firewall syslog message 106023 will be generated for packets denied by an ACE that does not have the **log** keyword present. Additional information about this syslog message is available at [Cisco Security Appliance System Log Message -- 106023](#). In the following examples, the **show logging | grep regex** command is used to extract syslog messages from the logging buffer on the firewall. It is possible to use different regex patterns with the **grep** keyword to search for specific data present within the logged messages.

```

firewall#: show logging | grep 106023
Mar 16 2007 20:58:35: %ASA-4-106023: Deny udp src outside:192.168.160.132/5158
dst inside:192.168.2.3/161
by access-group "outside"

```

In the preceding example, the message (106023) logged for tACL outside indicates a potential to exploit this vulnerability. The syslog output in this example is representative of what the messages would look like on each of the Cisco ASA, PIX, and FWSM firewall platforms.

## Cisco Intrusion Prevention System

### Identification

Beginning with signature update S70, IPS signature 4512 will trigger a low-severity alarm on potential attempts to exploit the default SNMP community strings vulnerability with a community string of *public*, which may indicate an attempt to gain control of the WLC. The following low-severity event was triggered on a Cisco IPS Sensor deployed in promiscuous mode. IPS Signature 4512 (Signature Name: SNMP Community String Public) triggers a low-severity alarm on potential attempts to exploit the vulnerability, which may indicate an attempt to take control of this platform. Because this signature triggers a low-severity event, customers may not see this event on the IPS monitoring consoles.

```

R4-IPS4240a# show events alert

evIdsAlert: eventId=1166754278236287354 severity=low vendor=Cisco
originator:
  hostId: R4-IPS4240a
  appName: sensorApp
  appInstanceId: 7007
time: 2007/04/09 19:37:04 2007/04/09 14:37:04 CDT
signature: description=SNMP Community String Public id=4512 version=S70
  subsigId: 0
  sigDetails: public
  marsCategory: Penetrate/GuessPassword/SNMP
interfaceGroup: vs0
vlan: 0

```

```

participants:
  attacker:
    addr: locality=OUT 64.101.135.167
    port: 1666
  target:
    addr: locality=OUT 192.168.2.3
    port: 161
    os: idSource=unknown relevance=relevant type=unknown
triggerPacket:
000000 00 18 74 7C 04 00 00 18 74 A2 0C 00 08 00 45 00 ..t|...t....E.
000010 00 98 55 A9 00 00 7A 11 E1 DF 40 65 87 A7 C0 A8 ..U...z...@e....
000020 80 17 06 82 00 A1 00 84 D9 64 30 7A 02 01 01 04 .....d0z....
000030 06 70 75 62 6C 69 63 A0 6D 02 01 01 02 01 00 02 .public.m.....
000040 01 00 30 62 30 0C 06 08 2B 06 01 02 01 01 01 00 ..0b0...+.....
000050 05 00 30 0C 06 08 2B 06 01 02 01 01 02 00 05 00 ..0...+.....
000060 30 0C 06 08 2B 06 01 02 01 01 03 00 05 00 30 0C 0...+.....0.
000070 06 08 2B 06 01 02 01 01 04 00 05 00 30 0C 06 08 ..+.....0...
000080 2B 06 01 02 01 05 00 05 00 30 0C 06 08 2B 06
+.....0...+.
000090 01 02 01 01 06 00 05 00 30 0C 06 08 2B 06 01 02 .....0...+...
0000A0 01 01 07 00 05 00 .....
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 55
  threatRatingValue: 55
  interface: ge0_0
  protocol: udp

```

Beginning with signature update S209, IPS signature 6003 will trigger a low-severity alarm on potential attempts to exploit the default SNMP community strings vulnerability with a community string of *private*, which may indicate an attempt to gain control of the WLC. The following low-severity event was triggered on a Cisco IPS Sensor deployed in promiscuous mode. IPS Signature 6003 (Signature Name: SNMP Community String Private) triggers a low-severity alarm on potential attempts to exploit the vulnerability, which may indicate an attempt to take control of this platform. Because this signature triggers a low-severity event, customers may not see this event on the IPS monitoring consoles.

### Signature: 6003/0 Showing the SNMP Community String Private Event

```

evIdsAlert: eventId=1166754278236279040 severity=low vendor=Cisco
originator:
  hostId: R4-IPS4240a
  appName: sensorApp
  appInstanceId: 7007
time: 2007/03/30 21:29:51 2007/03/30 16:29:51 CDT
signature: description=SNMP Community String Private id=6003 version=S209
  subsigId: 0
  sigDetails: private
  marsCategory: Penetrate/RetrievePassword/SNMP
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 192.168.208.63
    port: 32780
  target:
    addr: locality=OUT 192.168.2.3
    port: 161
    os: idSource=unknown relevance=relevant type=unknown
triggerPacket:
000000 00 18 74 7C 04 00 00 18 74 A2 0C 00 08 00 45 00 ..t|...t....E.
000010 00 46 00 00 40 00 3E 11 6B 13 C0 A8 D0 3F C0 A8 .F..@.>.k....?..
000020 80 03 80 0C 00 A1 00 32 A5 09 30 28 02 01 00 04 .....2..0(....
000030 07 70 72 69 76 61 74 65 A1 1A 02 04 60 13 D3 16 .private....`...
000040 02 01 00 02 01 00 30 0C 30 0A 06 06 2B 06 01 02 .....0.0...+...
000050 01 01 05 00 ....
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 42

```

```

threatRatingValue: 42
interface: ge0_0
protocol: udp

```

## Cisco Security Monitoring, Analysis, and Response System

### Identification: CS MARS Incident

A MARS incident will be triggered by rule "System Rule: Password Attack: SNMP – Attempt" when three events of the MARS class "Penetrate/GuessPassword/SNMP" are seen within 30 minutes. Signatures 4512/0 and 6003/0 trigger events with MARS class "Penetrate/GuessPassword/SNMP."

The "Incident Detail" display shown bellow was triggered by repeated attempts of exploiting the Default SNMP community strings vulnerability:

The screenshot displays the Cisco MARS Incident Details page. The browser title is "[R4-MARS] Incident Details - Microsoft Internet Explorer provided by Cisco Systems, Inc.". The address bar shows the URL: "https://10.88.226.42/incidents/IncidentDetails.jsp?Incident\_Id=13863107".

The page header includes the Cisco Systems logo and navigation tabs: SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, HELP. The current date and time are "Apr 9, 2007 5:06:31 PM CDT". The user is logged in as "Administrator (phadmin)".

The incident details section shows:

- Incident ID: 13863107
- Session ID: (empty)
- Rule Name: System Rule: Password Attack: SNMP - Attempt
- Action: None
- Description: This correlation rule detects attempts to retrieve SNMP community strings or access SNMP information by guessing SNMP community strings. Many SNMP installations have easily guessable passwords by default. The password attack may be preceded by reconnaissance attacks to the host.
- Status: Active
- Time Range: 0h:30m

The main table lists events related to this incident:

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close	Operation
1	(	ANY	SAME, TARGET01, ANY	ANY	Probe/HostInfo/All, Penetrate/ViewFiles/Sensitive	ANY	None	ANY	ANY	1		FOLLOWED-BY
2		ANY	SAME, TARGET01, ANY	ANY	Penetrate/RetrievePassword/SNMP, Penetrate/GuessPassword/SNMP	ANY	SAME, \$USER01	ANY	ANY	3	)	OR
3		ANY	SAME, TARGET01, ANY	ANY	Penetrate/RetrievePassword/SNMP, Penetrate/GuessPassword/SNMP	ANY	SAME, \$USER01	ANY	ANY	3		

Below the table, there are buttons for "Expand All" and "Collapse All".

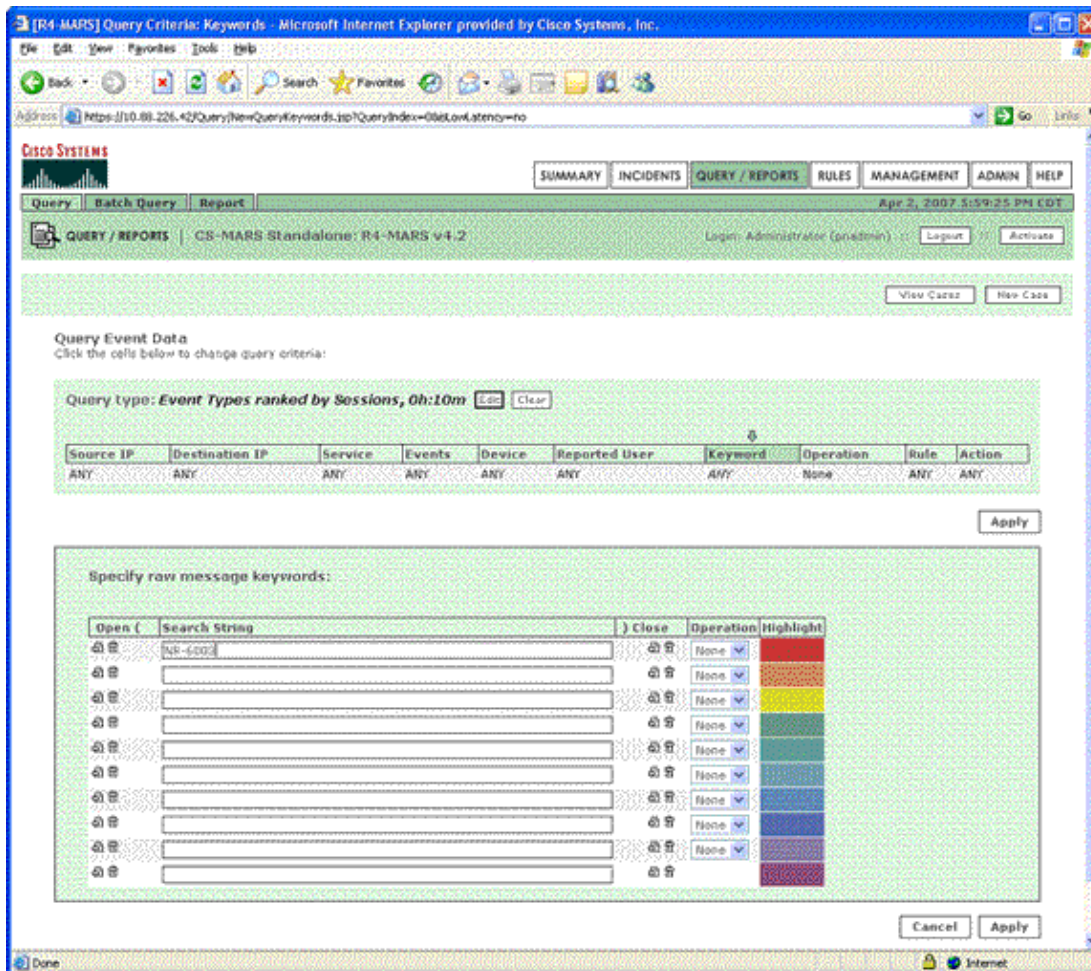
The incident ID is 13863107. The main table below shows event details:

Offset	Session / Incident ID	Event Type	Source IP / Port	Destination IP / Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
3		SNMP Read/Write Default/NULL Community String Used	192.168.208.63 32760	192.168.128.23 161	UDP	Apr 9, 2007 5:00:58 PM CDT	R4-IPS4240a			Total: 9

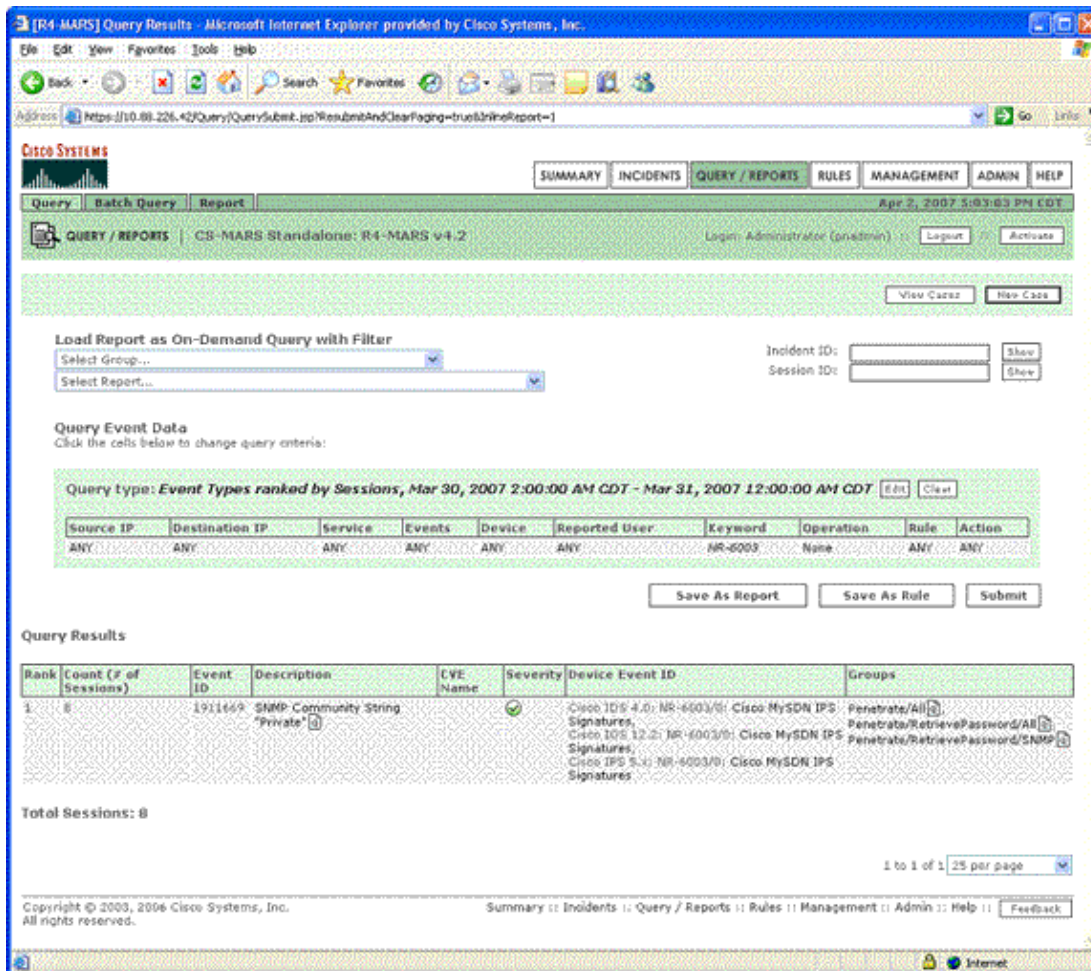
Copyright © 2003, 2006 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help :: Feedback

### Identification: CS MARS Keyword Query

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) console can be monitored for attempts to exploit the vulnerabilities described in this document. Using the query NR-6003 on the MARS appliance, will display events triggered by signature 6003/0:



The following display is the result of the query for IPS events triggered by signature 6003/0:



## Additional Information

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

## Revision History

Revision 1.0	2007-April-12	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](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

- [Infrastructure Protection Access Control Lists](#)
  - [Transit Access Control Lists](#)
  - [Configuring DHCP Features and IP Source Guard](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Apr 12, 2007

Document ID: 91288

---