

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco 10000, uBR10012, and uBR7200 Series Devices IPC Vulnerability and the Cisco uBR10012 Series Devices SNMP Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20080924-ipc-and-ubr.shtml>

Revision 1.0

For Public Release 2008 September 24 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 Advisories *Cisco 10000, uBR10012, uBR7200 Series Devices IPC Vulnerability* and *Cisco uBR10012 Series Devices SNMP Vulnerability* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

Cisco 10000, uBR10012, and uBR7200 Series Devices IPC Vulnerability: These devices contain a vulnerability when processing a UDP-based Inter-Process Communication (IPC) packet. This

vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may cause a crash of the affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service condition. The attack vector for exploitation is through an IPC packet using UDP destination port 1975. An attacker could exploit this vulnerability using spoofed packets.

This vulnerability has been assigned CVE identifiers CVE-2008-3805 and CVE-2008-3806.

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-20080924-ipc.shtml>.

Cisco uBR10012 Series Devices SNMP Vulnerability: This device exhibits a vulnerability when line card redundancy is enabled. When line card redundancy has been enabled, the device will automatically enable Simple Network Management Protocol (SNMP) with a community string of *private* that has Read and Write privileges to the device. This vulnerability can be exploited remotely with authentication and without end-user interaction. Successful exploitation of this vulnerability may allow complete control of the affected device or allow information disclosure, which could enable an attacker to learn information about the affected device and/or network. The attack vector for exploitation is through an SNMP packet using UDP port 161. An attacker could exploit this vulnerability using spoofed packets.

This vulnerability has been assigned CVE identifier CVE-2008-3807.

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-20080924-ubr.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)
- 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.

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:

- tACLs
- 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 these vulnerabilities.

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

Cisco IOS Software, Cisco ASA appliances, Cisco PIX security appliances, and FWSM firewalls can provide visibility through syslog messages and the counter values displayed in the output from **show** commands.

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 these vulnerabilities. Triage refers to sorting projects and prioritizing efforts that are most likely to be successful. Cisco has provided documents that can help organizations develop a risk-based triage capability for their information security teams. [Risk Triage for Security Vulnerability Announcements](#) and [Risk Triage and Prototyping](#) can help organizations develop repeatable security evaluation and response processes.

Device-Specific Mitigation and Identification



Caution: The effectiveness of any mitigation technique depends on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. As with any configuration change, evaluate the impact of this configuration prior to applying the change.

Specific information about mitigation and identification is available for these devices:

- [Cisco IOS Routers and Switches](#)
- [Cisco IOS NetFlow](#)
- [Cisco ASA, PIX, and FWSM Firewalls](#)
- [Cisco 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 IPC packets on UDP port 1975 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 any explicit permit statements for
!-- trusted sources that require access on the vulnerable ports.
!
!-- Note: IPC packets using UDP destination port 1975 are not
!-- permitted from any trusted source as this traffic
!-- should only be sent and received internally by the
!-- affected device using an IP address allocated from
!-- the 127.0.0.0/8 prefix.
!--
!-- IPC that traffic that is internally generated and
!-- sent and/or received by the affected device is not
!-- subjected to packet filtering by the applied iACL
!-- policy.
!

permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 161

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

deny udp any 127.0.0.0 0.255.255.255 eq 1975
deny udp any 192.168.60.0 0.0.0.255 eq 1975
deny udp any 192.168.60.0 0.0.0.255 eq 161

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

deny ip any 127.0.0.0 0.255.255.255
deny ip 127.0.0.0 0.255.255.255 any
```

```

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: Spoofing Protection

Unicast Reverse Path Forwarding

The vulnerabilities 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 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 IPC packets on UDP port 1975 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 udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq snmp (619 matches)
 20 deny udp any 127.0.0.0 0.255.255.255 eq 1975 (12 matches)
 30 deny udp any 192.168.60.0 0.0.0.255 eq 1975 (59 matches)
 40 deny udp any 192.168.60.0 0.0.0.255 eq 161 (82 matches)
 50 deny ip any 127.0.0.0 0.255.255.255
 60 deny ip 127.0.0.0 0.255.255.255 any
 70 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:

- **12 IPC** packets on **UDP destination port 1975** for ACE sequence identifier 20
- **59 IPC** packets on **UDP destination port 1975** for ACE sequence identifier 30
- **82 SNMP** packets on **UDP port 161** for ACE sequence identifier 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: 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, acl=0, drop=96, 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 self-ping
96 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           96        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
Frag: 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
      96 no route, 96 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 **96 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 the 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 (90784136 total packets):
  1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
  .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

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

IP Flow Switching Cache, 4456704 bytes
1885 active, 63651 inactive, 59960004 added
129803821 age polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
0 active, 16384 inactive, 0 added, 0 added to flow
0 alloc failures, 0 force free
1 chunk, 1 chunk added
last clearing of statistics never

```

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-Telnet	11393421	2.8	1	48	3.1	0.0	1.4
TCP-FTP	236	0.0	12	66	0.0	1.8	4.8
TCP-FTPD	21	0.0	13726	1294	0.0	18.4	4.1
TCP-WWW	22282	0.0	21	1020	0.1	4.1	7.3

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

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.10.201	Gi0/1	192.168.60.102	11	0984	00A1	17
Gi0/0	192.168.11.54	Gi0/1	192.168.60.158	11	0911	07B7	33
Gi0/1	192.168.150.60	Gi0/0	10.89.16.226	06	0016	12CA	1
Gi0/0	192.168.13.97	Gi0/1	192.168.60.28	11	0B3E	07B7	55
Gi0/0	192.168.10.17	Gi0/1	192.168.60.97	11	0B89	00A1	41
Gi0/0	10.88.226.1	Gi0/1	192.168.202.22	11	007B	007B	1
Gi0/0	192.168.12.185	Gi0/1	192.168.60.239	11	0BD7	00A1	19
Gi0/0	10.89.16.226	Gi0/1	192.168.150.60	06	12CA	0016	1
Gi0/0	192.168.11.131	Gi0/1	192.168.60.245	06	0B66	098C	18
Gi0/0	192.168.10.201	Gi0/1	192.168.60.102	11	0984	07B7	21
Gi0/0	192.168.1.230	Gi0/1	192.168.60.42	06	0C09	098C	23
Gi0/0	192.168.11.54	Gi0/1	192.168.60.158	11	0911	00A1	13
Gi0/1	192.168.150.60	Gi0/0	10.89.16.226	06	0016	12CA	1
Gi0/0	192.168.13.97	Gi0/1	192.168.60.28	11	0B3E	07B7	35
Gi0/0	192.168.11.230	Gi0/1	192.168.60.20	06	0C09	098C	72
Gi0/0	192.168.10.17	Gi0/1	192.168.60.97	11	0B89	00A1	81
Gi0/0	192.168.72.110	Gi0/1	192.168.60.118	06	092A	098C	44
Gi0/0	10.88.226.1	Gi0/1	192.168.202.22	11	007B	007B	1
Gi0/0	192.168.13.7	Gi0/1	192.168.60.162	06	0914	098C	21
Gi0/0	192.168.41.86	Gi0/1	192.168.60.27	06	0B7B	098C	11
Gi0/0	10.89.16.226	Gi0/1	192.168.150.60	06	12CA	0016	1

router#

In the preceding example, there are multiple flows for **IPC packets** on **UDP destination port 1975 (hex value 07B7)** and **SNMP packets** on **UDP port 161 (hex value 00A1)**. 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 IPC traffic sent on UDP port 1975 and SNMP traffic sent on UDP port 161 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

Note: IPC packets using UDP port 1975 should only be sent and received internally by the affected device using an IP address allocated from the 127.0.0.0/8 prefix.

To view only the traffic flows for IPC packets on UDP port 1975 (hex value 07B7) or SNMP packets on UDP port 161 (hex value 00A1), the command **show ip cache flow | include SrcIf|_11_.*(07B7|00A1)** will display the related UDP NetFlow records as shown here:

UDP Flows

```
router#show ip cache flow | include SrcIf|_11_.*(07B7|00A1)
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.10.201	Gi0/1	192.168.60.102	11	0984	00A1	1
Gi0/0	192.168.11.54	Gi0/1	192.168.60.158	11	0911	07B7	3
Gi0/0	192.168.13.97	Gi0/1	192.168.60.28	11	0B3E	07B7	5

Gi0/0	192.168.10.17	Gi0/1	192.168.60.97	11 0B89 00A1	4
Gi0/0	192.168.12.185	Gi0/1	192.168.60.239	11 0BD7 00A1	1
Gi0/0	192.168.10.201	Gi0/1	192.168.60.102	11 0984 07B7	2
Gi0/0	192.168.11.54	Gi0/1	192.168.60.158	11 0911 00A1	1
Gi0/0	192.168.13.97	Gi0/1	192.168.60.28	11 0B3E 07B7	3
Gi0/0	192.168.10.17	Gi0/1	192.168.60.97	11 0B89 00A1	8

router#

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Transit Access Control Lists

To protect the network from traffic that enters the network at ingress access points, which may include Internet connection points, partner and supplier connection points, or VPN connection points, administrators are advised to deploy tACLs to perform policy enforcement. Administrators can construct a tACL by explicitly permitting only authorized traffic to enter the network at ingress access points or permitting authorized traffic to transit the network in accordance with existing security policies and configurations. A tACL workaround cannot provide complete protection against these vulnerabilities when the attack originates from a trusted source address.

The tACL policy denies unauthorized IPC packets on UDP port 1975 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](#).

```

!
!-- When applicable, include any explicit permit statements for
!-- trusted sources that require access on the vulnerable ports
!
!-- Note: IPC packets using UDP destination port 1975 are not
!-- permitted from any trusted source as this traffic
!-- should only be sent and received internally by the
!-- affected device using an IP address allocated from
!-- the 127.0.0.0/8 prefix.
!--
!-- IPC that traffic that is internally generated and
!-- sent and/or received by the affected device is not
!-- subjected to packet filtering by the applied iACL
!-- policy.
!

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 udp any 192.168.60.0 255.255.255.0 eq 197
access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq 161

!

```

```

!-- 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

The vulnerabilities described in this document can be exploited by spoofed IP packets. Administrators can deploy and configure 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 IPC packets on UDP port 1975 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; 4 elements
access-list tACL-Policy line 1 extended permit udp host 192.168.100.1 192.168.6
access-list tACL-Policy line 2 extended deny udp any 192.168.60.0 255.255.255.0
access-list tACL-Policy line 3 extended deny udp any 192.168.60.0 255.255.255.0
access-list tACL-Policy line 4 extended deny ip any any (hitcnt=8)
firewall#

```

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

- **91 IPC** packets on **UDP destination port 1975** for ACE line 2
- **38 SNMP** packets on **UDP port 161** for ACE line 3

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 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
Aug 18 2008 00:15:13: %ASA-4-106023: Deny udp src outside:192.168.10.18/2944
dst inside:192.168.60.191/161 by access-group "tACL-Policy"
Aug 18 2008 00:15:13: %ASA-4-106023: Deny udp src outside:192.168.11.200/2945
dst inside:192.168.60.33/161 by access-group "tACL-Policy"
Aug 18 2008 00:15:13: %ASA-4-106023: Deny udp src outside:192.168.19.99/2946
dst inside:192.168.60.240/1975 by access-group "tACL-Policy"
Aug 18 2008 00:15:13: %ASA-4-106023: Deny udp src outside:192.168.17.100/2947
dst inside:192.168.60.115/1975 by access-group "tACL-Policy"
Aug 18 2008 00:15:13: %ASA-4-106023: Deny udp src outside:192.168.12.88/2949
dst inside:192.168.60.38/161 by access-group "tACL-Policy"
Aug 18 2008 00:15:13: %ASA-4-106023: Deny udp src outside:192.168.24.175/2950
dst inside:192.168.60.250/1975 by access-group "tACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *tACL-Policy* show **IPC** packets on **UDP port 1975** and **SNMP** packets on **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: 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 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
Aug 18 2008 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
192.168.60.1 to 192.168.60.100 on interface outside
Aug 18 2008 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
192.168.60.1 to 192.168.60.100 on interface outside
Aug 18 2008 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          11
firewall#
```

In the preceding example, Unicast RPF has dropped **11 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 the Cisco Intrusion Prevention System (IPS) appliances and services modules to provide threat detection and help prevent attempts to exploit the *Cisco uBR10012 Series Devices SNMP Vulnerability* described in this document. Beginning with signature update S209 for sensors running Cisco IPS version 6.x or 5.x, this vulnerability can be detected by signature 6003/0 (Signature Name: SNMP Community String Private). Signature 6003/0 is not enabled by default, triggers a *Low* severity event, has a signature fidelity rating (SFR) of 75, and is configured with a default event action of **produce-alert**.

Signature 6003/0 will fire if the community string *private* is detected in an SNMP request. Firing of this signature may indicate potential exploitation of the *Cisco uBR10012 Series Devices SNMP 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 vulnerability that is 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 vulnerability that is 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: 6003/0 - SNMP Community String Private

```
ips-sensor# show events alert | include id=6003
evIdsAlert: eventId=1212721493148092748 severity=low vendor=Cisco
  originator:
    hostId: ips-sensor
    appName: sensorApp
    appInstanceId: 418
  time: 2008/08/21 21:02:25 2008/08/21 16:02:25 CDT
  signature: description=SNMP Community String Private id=6003 version=S209
    subsigId: 0
    sigDetails: private
    marsCategory: Penetrate/RetrievePassword/SNMP
  interfaceGroup: vs0
  vlan: 203
  participants:
    attacker:
      addr: locality=OUT 192.168.11.200
      port: 32779
    target:
      addr: locality=IN 192.168.60.100
      port: 161
      os: idSource=unknown relevance=relevant type=unknown
  triggerPacket:
000000  D0 E0 00 00 A0 D0 0B 0A 0D 0A 05 05 08 00 45 00  .....E.
000010  00 45 00 00 40 00 3F 11 72 2B C0 A8 0B C8 C0 A8  .E..@.?.r+.....
000020  3C 64 80 0B 00 A1 00 31 A2 C6 30 27 02 01 01 04  <d.....1..0'....
000030  07 70 72 69 76 61 74 65 A1 19 02 04 27 C0 19 C8  .private....'...
000040  02 01 00 02 01 00 30 0B 30 09 06 05 2B 06 01 02  .....0.0...+...
000050  01 05 00                                     ...
    riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 42
    threatRatingValue: 42
  interface: ge0_0
  protocol: udp

ips-sensor#
```

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 vulnerability that is described in this document using IPS signature 6003/0 (Signature Name: SNMP Community String Private). After the S209 dynamic signature update has been downloaded, using keyword **NR-6003/0** for IPS signature 6003/0 and a query type of **All Matching Event Raw Messages** on the Cisco Security MARS appliance will provide a report that lists the incidents created by the IPS signature.

The following screen shot shows the actual incident created by IPS signature 6003/0 (Signature Name: SNMP Community String Private):

The screenshot displays the configuration for a rule named 'System Rule: Password Attack: SNMP - Attempt'. The rule is active and has a time range of 0h:30m. The description states: '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.'

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close	Operation
1	(ANY	SAME, \$TARGETDL, ANY	ANY	Probe/HostInfo/All, Penetrate/ViewFiles/Sensitive	ANY	None	ANY	ANY	1		FOLLOWED-BY

Offset	Session	Incident	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close	Operation
					SNMP Community String "Private"	192.168.11.200	32779				161		
		S:476615577, I:475885814			SNMP Community String "Private"	192.168.11.200	32779				161		
		S:476616932, I:475885814			SNMP Community String "Private"	192.168.11.200	32779				161		
		S:476617550, I:475885814			SNMP Community String "Private"	192.168.11.200	32779				161		

The following screen shot shows the values used to query for events that are created by the IPS signature related to the *Cisco uBR10012 Series Devices SNMP Vulnerability*:

Query Event Data

Click the cells below to change query criteria:

Query type: **Event Raw Messages ranked by Time, 0h:45m**

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-6003/0	None	ANY	ANY

Specify raw message keywords:

Open (Search String) Close	Operation	Highlight
<input type="button" value="Add"/> <input type="button" value="Remove"/>	NR-6003/0	<input type="button" value="Add"/> <input type="button" value="Remove"/>	None	
<input type="button" value="Add"/> <input type="button" value="Remove"/>	NR-6003/0	<input type="button" value="Add"/> <input type="button" value="Remove"/>		
<input type="button" value="Add"/> <input type="button" value="Remove"/>		<input type="button" value="Add"/> <input type="button" value="Remove"/>	None	
<input type="button" value="Add"/> <input type="button" value="Remove"/>		<input type="button" value="Add"/> <input type="button" value="Remove"/>	None	
<input type="button" value="Add"/> <input type="button" value="Remove"/>		<input type="button" value="Add"/> <input type="button" value="Remove"/>	None	
<input type="button" value="Add"/> <input type="button" value="Remove"/>		<input type="button" value="Add"/> <input type="button" value="Remove"/>	None	
<input type="button" value="Add"/> <input type="button" value="Remove"/>		<input type="button" value="Add"/> <input type="button" value="Remove"/>	None	
<input type="button" value="Add"/> <input type="button" value="Remove"/>		<input type="button" value="Add"/> <input type="button" value="Remove"/>	None	

The following screen shot shows the query results for the *Cisco uBR10012 Series Devices SNMP Vulnerability* that are created by the Cisco Security MARS appliance:

Query type: **Event Raw Messages ranked by Time, 0h:45m**

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-6003/0	None	ANY	ANY

Query Results

Event / Session / Incident ID	Event Type	Time	Reporting Device	Raw Message	Path / Mitigation	Tune
E:476617550, S:476617550, I:475885814	SNMP Community String "Private"	Aug 21 2008 4:02 CDT	R4-	192.168.11.200/32779 --> 192.168.60.100/161 UDP SNMP Community String "Private", Time:1219352545,Risk Rating:42,VLAN:203,Port List:,161		False Positive Tuning
E:476616932, S:476616932, I:475885814	SNMP Community String "Private"	Aug 20 2008 3:52 CDT		192.168.11.200/32779 --> 192.168.60.100/161 UDP SNMP Community String "Private", Time:1219352341,Risk Rating:42,VLAN:203,Port List:,161		False Positive Tuning
E:476615577, S:476615577, I:475885814	SNMP Community String "Private"	Aug 20 2008 3:52 CDT		192.168.11.200/32779 --> 192.168.60.100/161 UDP SNMP Community String "Private", Time:1219351973,Risk Rating:42,VLAN:203,Port List:,161		False Positive Tuning

of 3

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 1.0	2008-September-24	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](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider](#)
- [Cisco 6.x Intrusion Prevention System](#)
- [Cisco IPS 6.x Signature Downloads](#)
- [Cisco IPS Signature Search Page](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)
- [Common Vulnerabilities and Exposures \(CVE\)](#) 

Help us help you.

Please rate this document.

- Excellent
 Good
 Average
 Fair
 Poor

This document solved my problem.

- Yes
 No
 Just browsing

Suggestions for improvement:

(256 character limit)

Send

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

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)