

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of Multiple Vulnerabilities in Cisco ASA/PIX/FWSM Firewalls

<http://www.cisco.com/warp/public/707/cisco-amb-20070214-firewall.shtml>

Revision 1.0

For Public Release 2007 February 14 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

Vulnerability Characteristics

Multiple vulnerabilities exist within Cisco PIX, ASA and FWSM products. Most of the vulnerabilities may result in a Denial of Service (DoS) condition, while one vulnerability results in privilege escalation and one has the potential for remote code execution. With the exception of the local privilege escalation vulnerability, all vulnerabilities can be exploited remotely without authentication or user interaction. The following information provides a vulnerability summary.

- Malformed Hypertext Transfer Protocol (HTTP) request DoS vulnerability (Cisco Bug ID CSCsd75794): Cisco PIX, ASA, and FWSM products are affected. The likely attack vector is TCP port 80 traffic that transits the device.
- Malformed Session Initiation Protocol (SIP) messages DoS vulnerability (Cisco Bug ID CSCsg80915, CSCse27708, CSCsd97077): Cisco PIX, ASA, and FWSM products are affected. The likely attack vector is UDP port 5060. An attacker could use spoofed packets to exploit the vulnerability.

- Malformed auth-proxy requests using Secure Hypertext Transfer Protocol (HTTPS) DoS vulnerability (Cisco Bug ID CSCsg50228): The FWSM product is affected. The likely attack vector is TCP port 443. This is configuration dependent and will not be covered in this document.
- Long auth-proxy request vulnerability (Cisco Bug ID CSCsd91268): The FWSM product is affected. This could result in a DoS or potentially remote code execution. Likely attack vectors are TCP ports 80 and 443. This is configuration dependent and will not be covered in this document. Device Directed packet processing DoS vulnerability (Cisco Bug ID CSCse85707): The FWSM product is affected.
- Device Directed Secure Hypertext Transfer Protocol (HTTPS) processing DoS vulnerability (Cisco Bug ID CSCsf29974): The FWSM product is affected. The likely attack vector is TCP port 443.
- Malformed SNMP request DoS vulnerability (Cisco Bug ID CSCse52679): The FWSM product is affected. The likely attack vector is UDP port 161. An attacker could use spoofed packets to exploit the vulnerability.
- Malformed TCP Packet DoS vulnerability (Cisco Bug ID CSCsh12711): The Cisco ASA and PIX Firewall products are affected. The attack vector is an inspected TCP stream.
- Local Privilege Escalation Vulnerability (Cisco Bug ID CSCsh33287): This is configuration dependent and will not be covered in this document.
- Access Control List (ACL) Corruption vulnerability. This is configuration dependent and will not be covered in this document.

This document contains information to assist Cisco customers in detecting and mitigating attempts to exploit Multiple Denial of Service Vulnerabilities in Cisco FWSM, PIX and ASA Firewalls.

Vulnerable, unaffected, and fixed software information is available in the following PSIRT Security Advisories:

<http://www.cisco.com/warp/public/707/cisco-sa-20070214-fwsm.shtml>

<http://www.cisco.com/warp/public/707/cisco-sa-20070214-pix.shtml>

Mitigation Technique Overview

Cisco devices provide several countermeasures for the Multiple Cisco PIX, ASA and FWSM vulnerabilities. The most preventive controls are provided by applying configuration changes directly to the affected devices as detailed in the associated PSIRT advisories. ACLs on screening devices can offer mitigation and provide defense in depth for some of the vulnerabilities. Cisco Intrusion Prevention System (IPS) provides detective controls, and potential mitigation for certain vulnerabilities. NetFlow can be used as a tool to aid in detection. Flexible Packet Matching (FPM) can be used to provide mitigation for one vulnerability. The following provides a summary of vulnerability mitigation techniques available.

- Malformed Hypertext Transfer Protocol (HTTP) request DoS vulnerability (Cisco Bug ID CSCsd75794): This vulnerability can be prevented through configuration changes directly to the affected device. These changes can reduce the security of protected endpoint devices, however there will still be some HTTP specific protocol protection in place. Cisco Secure Intrusion Prevention System can detect and mitigate this vulnerability with IPS signature 5284/0 from signature pack 271.
- Malformed Session Initiation Protocol (SIP) messages DoS vulnerability (Cisco Bug ID CSCsg80915, CSCse27708, CSCsd97077): The most preventive control is provided though disabling SIP inspection on the affected device, however this could negatively impact allowed SIP traffic. Threat exposure can be reduced by limiting SIP inspection to trusted devices and utilizing antispoofing capabilities. Cisco Secure Intrusion Prevention System can detect and

- potentially mitigate the vulnerability through IPS signature 5285/0 from signature pack 271.
- Device directed packet processing DoS vulnerability (Cisco Bug ID CSCse85707): This vulnerability can be prevented by changing the logging level of log message 710006. Infrastructure ACLs on screening devices can provide effective mitigation from untrusted sources. Flexible Packet Matching (FPM) can provide effective mitigation, although ACLs are more efficient. NetFlow, classification ACLs, and FPM can aid in detection of attempts to exploit this vulnerability. Several IPS signatures (1007,1109,1108,1101) can detect non standard protocol usage.
 - Device directed Secure Hypertext Transfer Protocol (HTTPS) processing DoS vulnerability (Cisco Bug ID CSCsf29974): This vulnerability can be prevented through configuration changes applied directly to the device. Access Control Lists (ACLs) on screening devices to allow only trusted traffic can provide effective mitigation from untrusted sources.
 - Malformed SNMP request DoS vulnerability (Cisco Bug ID CSCse52679): This vulnerability can be prevented by applying configuration changes directly to the device if SNMP is not required. IPS signature 4508/0 from signature pack S43 can identify attempts to exploit the vulnerability though it may not provide complete coverage. Since a vulnerable configuration will specify access control, ACLs on screening devices only provide additional defense in depth protection. Since SNMP is sessionless, this vulnerability can be exploited by spoofed packets that arrive on the expected interface. Antispoofing capabilities deployed throughout the network can reduce the likelihood of spoofed packet exploitation as well as aid in attack traceback.
 - Malformed TCP Packet DoS vulnerability (Cisco Bug ID CSCsh12711): This vulnerability can be prevented through configuration changes applied directly to the device. Cisco Secure Intrusion Prevention System can detect and mitigate this vulnerability with IPS signature 5237/0 from signature pack 271.

Device-Specific Mitigation and Identification

- [Internet Edge Routers](#)
- [Cisco ASA, PIX and FWSM Firewalls](#)
- [Cisco IOS Switches](#)
- [Cisco Intrusion Prevention System](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)

Internet Edge Routers



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

Mitigation: Infrastructure Access Control Lists (iACLs)

Infrastructure ACLs (iACLs) can be used as effective mitigation for the FWSM directed packet processing DoS (Cisco Bug ID CSCse85707) and the HTTPS processing DoS (Cisco Bug ID CSCsf29974) vulnerabilities, as well as provide an extra layer of protection for the malformed SNMP DoS (Cisco Bug ID CSCse52679).

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The ACL example shown below should be included as part of the deployed infrastructure access list which will protect all devices with IP addresses in the infrastructure IP address range.

In the following example, the address block 192.168.131.0/24 is infrastructure address space. Care should be taken to allow required traffic for routing or administrative access prior to denying all infrastructure directed traffic. Added access list entries should be implemented as part of a infrastructure ACL that filters traffic at network ingress points. For more information on infrastructure ACLs, refer to [Protecting Your Core: Infrastructure Protection Access Control Lists](#).

```

!-- Permit additional Layer 3 and Layer 4 traffic destined for infrastru
!-- address space as dictated by existing security policies and configuratio
!-- Permit/deny to infrastructure IP addresses in accordance with security p

!-- Vulnerability-specific deny to aid identification SNMP DoS(CSCse52679)

access-list 150 deny udp any 192.168.131.0 0.0.0.255 eq 161

!-- Vulnerability-specific deny to aid identification HTTPS DoS(CSCsf29974)

access-list 150 deny tcp any 192.168.131.0 0.0.0.255 eq 443

!-- Default Deny to infrastructure IP addresses
!-- Vulnerability-specific deny to aid identification FWSM Directed packet
!-- --DoS(CSCse85707)

access-list 150 deny ip any 192.168.131.0 0.0.0.255

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

interface GigabitEthernet 0/0
ip access-group 150 in

```

Mitigation: Flexible Packet Matching (FPM)

Flexible Packet Matching (FPM) was introduced in 12.4(4)T and has the capability to deny specific packets based on content within the first 256 bytes of the packet. The [Flexible Packet Matching Deployment Guide](#) contains further information on FPM. In this specific case FPM can be an effective means to block unwanted activity directed at a FWSM interface. FPM is more processor intensive than an ACL and therefore, if the strategies provide equal protection an ACL should be used if possible. For this vulnerability, a properly constructed ACL will provide equal protection and is a preferable method for mitigation. FPM, however, may provide better identification capabilities.

In the following example, the vulnerable FWSM device interface is at IP address 192.168.131.10. This will need to be changed to addresses within your network. Since protocols ICMP , IGMP , TCP , ESP , OSPF ,PIM and Failover do not cause the vulnerability all other protocols should be dropped. Since the FWSM device does not use other protocols, there is no reason for any other protocols to target an FWSM device.

```
(config)#class-map type access-control match-any ip
(config-cmap)#description "target address"
(config-cmap)#match field ip dest-addr eq 192.168.131.10

(config)#class-map type access-control match-any vulnprotos
(config-cmap)#description "protocols that trigger vulnerability"
(config-cmap)#match field ip protocol gt 105
(config-cmap)#match field ip protocol range 90 104
(config-cmap)#match field ip protocol range 51 88
(config-cmap)#match field ip protocol range 18 49
(config-cmap)#match field ip protocol range 7 16
(config-cmap)#match field ip protocol range 3 5

(config)#policy-map type access-control fwsml_directed
(config-pmap)#description "policy to deny specific protocols"
(config-pmap)#class vulnprotos
(config-pmap-c)#drop

(config)#policy-map type access-control fpm_policy
(config-pmap)#description "drop_vulnerable_protocols"
(config-pmap)#class ip
(config-pmap-c)#service-policy fwsml_directed

(config)#interface gigabitEthernet 0/0
(config-if)#service-policy type access-control input fpm_policy
```

Mitigation: Anti-Spoofing

The SNMP DoS vulnerability, SIP vulnerability, and FWSM directed packet DoS can be exploited by spoofed packets. Antispoofing protection in the form of unicast Reverse Path Forwarding (uRPF) can provide limited mitigation if properly configured. This feature should not be relied upon to provide 100% mitigation since spoofed packets may still enter the network from the interface expected by uRPF. Care must be taken to ensure that the appropriate uRPF mode (loose or strict) is configured to ensure that legitimate packets are not dropped. Additional information about unicast Reverse Path Forwarding is available at

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_urpf.html.

Identification: Infrastructure Access Control Lists (iACLs)

After the interface ACL is applied to the ingress interface, the command **show access-list *acl-number*** can be used to identify the number of packets being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit a vulnerability. The following is an example of output for the **show access-list 150** command configured inbound on interface GigabitEthernet 0/0.

```
show access-lists 150
Extended IP access list 150

! -- Potentially Malformed SNMP DoS(CSCse52679)

10 deny udp any 192.168.131.0 0.0.0.255 eq snmp (3 matches)

! -- Potentially Malformed HTTPS DoS(CSCsf29974)
```

```

20 deny tcp any 192.168.131.0 0.0.0.255 eq 443 (3 matches)
! -- Potentially FWSM Directed Packet DoS(CSCse85707) or other unrelated tra
30 deny ip any 192.168.131.0 0.0.0.255 (124 matches)

```

In the above example, three UDP/161, three TCP/443 and 124 IP packets have been dropped by access-list 150.

Identification: Flexible Packet Matching

FPM can give detailed statistics of policy infractions.

```

#show policy-map type access-control interface gigabitEthernet 0/0
drop
GigabitEthernet0/0

Service-policy access-control input: fpm_policy

Class-map: ip (match-any)
  511 packets, 30660 bytes
  5 minute offered rate 0 bps
  Match: field IP dest-addr eq 192.168.131.10

Service-policy access-control : fwsmdirected

Class-map: vulnprotos (match-any)
  496 packets, 29760 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: field IP protocol gt 105
    304 packets, 18240 bytes
    5 minute rate 0 bps
  Match: field IP protocol range 90 104
    26 packets, 1560 bytes
    5 minute rate 0 bps
  Match: field IP protocol range 51 88
    76 packets, 4560 bytes
    5 minute rate 0 bps
  Match: field IP protocol range 18 49
    64 packets, 3840 bytes
    5 minute rate 0 bps
  Match: field IP protocol range 7 16
    20 packets, 1200 bytes
    5 minute rate 0 bps
  Match: field IP protocol range 3 5
    6 packets, 360 bytes
    5 minute rate 0 bps

```

In the above example, we can see that a total of 496 packets were dropped by the FPM policy. These dropped packets can be further identified as follows:

- 304 packets using an IP protocol greater than 105
- 26 packets using an IP protocol between 90 and 104
- 76 packets using an IP protocol between 51 and 88
- 64 Packets using an IP protocol between 18 and 49
- 20 Packets using an IP protocol between 7 and 16
- 6 Packets using an IP protocol between 3 and 5

Identification: NetFlow

NetFlow can be configured on Internet Edge routers and switches to determine if attempts are in progress to exploit these vulnerabilities. Attempts to exploit the FWSM directed packet DoS (Cisco Bug ID CSCse85707) are likely to use protocols other than TCP, UDP, ICMP destined to infrastructure address space. Attempts to exploit the SNMP DoS (Cisco Bug ID CSCse52679) vulnerability are likely to show connections destined to infrastructure address space destined for port UDP/161. Attempts to exploit the malformed HTTPS DoS (Cisco Bug ID CSCsf29974) are likely to show HTTPS connections directed to infrastructure address space. This first example has a high amount of IP-Other protocols as well as IPv6INIP and IPINIP protocols which may be attempts to exploit the FWSM directed packet DoS.

```
#show ip cache flow
```

```
IP packet size distribution (4401773 total packets):
```

```
 1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 48
    .003 .818 .060 .031 .006 .015 .000 .005 .000 .000 .005 .000 .000 .000 .00
    512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
    .000 .000 .020 .003 .023 .000 .000 .000 .000 .000 .000
```

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

```
 13 active, 65523 inactive, 164081 added
 2848812 ager polls, 0 flow alloc failures
 Active flows timeout in 30 minutes
 Inactive flows timeout in 15 seconds
```

```
IP Sub Flow Cache, 336520 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 | Flows /Sec | Packets /Flow | Bytes /Pkt | Packets /Sec | Active(Sec) /Flow | Idle(Se /Flow |
|-----------------|----------------|---------------|------------------|---------------|-----------------|----------------------|------------------|
| TCP-Telnet | 407 | 0.0 | 90 | 52 | 0.0 | 34.4 | 12.6 |
| TCP-FTP | 55 | 0.0 | 4 | 66 | 0.0 | 4.3 | 10.9 |
| TCP-FTPD | 22 | 0.0 | 19673 | 41 | 0.1 | 1157.2 | 4.4 |
| TCP-WWW | 3035 | 0.0 | 122 | 58 | 0.1 | 5.9 | 11.8 |
| TCP-SMTP | 6 | 0.0 | 1 | 44 | 0.0 | 0.0 | 15.3 |
| TCP-X | 6 | 0.0 | 1 | 44 | 0.0 | 0.0 | 15.5 |
| TCP-BGP | 6 | 0.0 | 1 | 44 | 0.0 | 0.0 | 15.9 |
| TCP-NNTP | 6 | 0.0 | 1 | 44 | 0.0 | 0.0 | 15.3 |
| TCP-Frag | 2 | 0.0 | 1 | 20 | 0.0 | 0.0 | 15.7 |
| TCP-other | 36728 | 0.0 | 85 | 84 | 1.0 | 4.4 | 6.8 |
| UDP-DNS | 708 | 0.0 | 1 | 67 | 0.0 | 0.7 | 15.4 |
| UDP-NTP | 44960 | 0.0 | 1 | 75 | 0.0 | 0.0 | 15.5 |
| UDP-TFTP | 5 | 0.0 | 1 | 28 | 0.0 | 0.0 | 15.6 |
| UDP-Frag | 1 | 0.0 | 1 | 20 | 0.0 | 0.0 | 15.7 |
| UDP-other | 45541 | 0.0 | 6 | 446 | 0.0 | 0.7 | 15.4 |
| ICMP | 27856 | 0.0 | 2 | 56 | 0.0 | 11.3 | 15.5 |
| IGMP | 18 | 0.0 | 2 | 20 | 0.0 | 0.7 | 15.4 |
| IPINIP | 17 | 0.0 | 2 | 20 | 0.0 | 1.1 | 15.4 |
| IPv6INIP | 18 | 0.0 | 2 | 20 | 0.0 | 1.7 | 15.5 |
| GRE | 20 | 0.0 | 1 | 20 | 0.0 | 0.2 | 15.4 |
| IP-other | 4653 | 0.0 | 1 | 20 | 0.0 | 0.5 | 15.5 |
| Total: | 164070 | 0.0 | 26 | 100 | 1.4 | 3.4 | 13.4 |

| SrcIf | SrcIPAddress | DstIf | DstIPAddress | Pr | SrcP | DstP | Pk |
|-------|----------------|-------|----------------|----|------|------|----|
| Gi0/0 | 192.168.208.63 | Null | 192.168.131.10 | A2 | 0000 | 0000 | |
| Gi0/0 | 192.168.208.63 | Null | 192.168.131.10 | E8 | 0000 | 0000 | |
| Gi0/0 | 192.168.208.63 | Gi0/0 | 10.82.209.27 | 06 | 0016 | 0EAD | |
| Gi0/0 | 192.168.208.63 | Gi0/0 | 10.82.209.27 | 06 | 0016 | 0EAC | |
| Gi0/0 | 192.168.208.63 | Null | 192.168.131.10 | 4D | 0000 | 0000 | |
| Gi0/0 | 192.168.208.63 | Null | 192.168.131.10 | 51 | 0000 | 0000 | |
| Gi0/0 | 192.168.208.63 | Null | 192.168.131.10 | 59 | 0000 | 0000 | |
| Gi0/0 | 192.168.208.63 | Null | 192.168.131.10 | 65 | 0000 | 0000 | |

The following example shows flows destined to port 443(Hex 01BB) and 161 (Hex 00A1)

```
show ip cache flow | include SrcIf | 00A1 | 01BB
SrcIf          SrcIPaddress      DstIf          DstIPaddress    Pr  SrcP  DstP  Pk
Gi0/0         192.168.208.63    Null          192.168.131.10  06  81F8  01BB
Gi0/0         192.168.208.63    Null          192.168.131.10  11  F272  00A1
```

Cisco ASA, PIX and FWSM Firewalls



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

Cisco ASA and PIX

Many networks are likely to have ASA, PIX or FWSM devices screening other ASA, PIX or FWSM devices located elsewhere within the network and providing defense in depth. The following examples are to be used when one of the aforementioned devices is providing access control for another vulnerable device. These examples are not meant to provide protection on the device that the mitigation techniques are implemented. For endpoint device specific mitigations, please refer to the PSIRT Security Advisories referenced in the Vulnerability Overview section.

Mitigation: Transit Access Control Lists (tACLs)

ACLs can be used as effective mitigation for the FWSM directed packet processing DoS (Cisco Bug ID CSCse85707) and the HTTPS processing DoS (Cisco Bug ID CSCsf29974) vulnerabilities as well as provide an extra layer of protection for the malformed SNMP DoS (Cisco Bug ID CSCse52679). The following example, is for a Firewall located near the network edge and therefore makes use of ACLs to deny all access to infrastructure address space. Care should be taken to allow required traffic for routing or administrative access prior to denying all infrastructure directed traffic.

For more information on transit ACLs, refer to

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml.

```
!-- Network Infrastructure Traffic permitted from outside network edge (Rout
!-- Vulnerability-specific deny to aid identification SNMP DoS(CSCse52679)

access-list TRANSIT extended deny udp any 192.168.131.0 255.255.255.0 eq snmp

!-- Vulnerability-specific deny to aid identification HTTPS DoS(CSCsf29974)

access-list TRANSIT extended deny tcp any 192.168.131.0 255.255.255.0 eq http

!-- Default deny to infrastructure IP addresses
!-- Vulnerability-specific deny to aid identification FWSM Directed Packet
! --DoS(CSCse85707)

access-list TRANSIT extended deny ip any 192.168.131.0 255.255.255.0
```

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

```
!-- Apply tACL to outside interface in the inbound direction
```

```
access-group TRANSIT in interface outside
```

Mitigation: AntiSpoofing

The SNMP DoS vulnerability and FWSM directed packet DoS can be exploited by spoofed packets. Antispoofing protection in the form of unicast Reverse Path Forwarding (uRPF) can provide limited mitigation if properly configured. This feature should not be relied upon to provide 100% mitigation since spoofed packets may still enter the network from the interface expected by uRPF or allowed by anti-spoofing access-lists. Also care must be taken to ensure that the appropriate uRPF mode (loose or strict) is configured to ensure that legitimate packets are not dropped. Additional information about unicast Reverse Path Forwarding is available at the following URL <http://www.cisco.com/en/US/docs/security/asa/asa70/system/message/logmsgs.html#wp1279875>.

Identification: Access Control Lists (ACLs)

After the transit ACL is applied to the ingress interface, the command **show access-list** *acl-name* can be used to identify the number of packets being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit a vulnerability. The following is an example of output for the **show access-list TRANSIT** command.

```
#show access-list TRANSIT
access-list TRANSIT; 3 elements

! -- Potential SNMP DoS (CSCse52679)

access-list TRANSIT line 1 extended deny udp any 192.168.131.0 255.255.255.0

! -- Potential HTTP DoS (CSCsf29974)

access-list TRANSIT line 2 extended deny tcp any 192.168.131.0 255.255.255.0

! -- Potentially FWSM Directed packet DoS(CSCse85707) or other unrelated tra.

access-list TRANSIT line 3 extended deny ip any 192.168.131.0 255.255.255.0
```

In the above example, two UDP/161, two TCP/443 and 490 IP packets have been dropped by the ACL configured on the outside interface.

Identification: Syslog Messages

Syslog Message 106021 will aid in the identification of potential spoofing attempts.

<http://www.cisco.com/en/US/docs/security/asa/asa70/system/message/logmsgs.html#wp1279871>

In access lists where no logging keyword was added to the ACL, syslog message 106023 will be generated. For more information on the specific message, refer to [Cisco Security Appliance System](#)

[Log Message 106023](#).

Information on configuring syslog for the ASA Firewall appliance is available in [Configuring Logging on the Security Appliance](#).

Firewall Services Module

Mitigation: Transit Access Control Lists (tACLs)

ACLs can be used as effective mitigation for the FWSM directed packet processing DoS (Cisco Bug ID CSCse85707) and the HTTPS processing DoS (Cisco Bug ID CSCsf29974) vulnerabilities as well as provide an extra layer of protection for the malformed SNMP DoS (Cisco Bug ID CSCse52679). The following example, is for a FWSM located near the network edge and makes use of ACLs to deny all access to infrastructure address space. Care should be taken to allow required traffic for routing or administrative access prior to denying all infrastructure directed traffic.

For more information on infrastructure ACLs, refer to

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml.

```

!-- Network Infrastructure Traffic permitted from outside network edge (Rout
!-- Vulnerability-specific deny to aid identification SNMP DoS(CSCse52679)

access-list TRANSIT extended deny udp any 192.168.131.0 255.255.255.0 eq snmp

!-- Vulnerability-specific deny to aid identification HTTPS DoS(CSCsf29974)

access-list TRANSIT extended deny tcp any 192.168.131.0 255.255.255.0 eq http

!-- Default deny to infrastructure IP addresses
!-- Vulnerability-specific deny to aid identification FWSM Directed Packet
!-- --DoS(CSCse85707)

access-list TRANSIT extended deny ip any 192.168.131.0 255.255.255.0

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

!-- Apply tACL to outside interface in the inbound direction

access-group TRANSIT in interface outside

```

Identification: Access Control Lists (ACLs)

After the transit ACL is applied to the ingress interface, the command **show access-list acl-name** can be used to identify the number of packets being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit a vulnerability. The following is an example of output for the **show access-list TRANSIT** command.

```
#show access-list TRANSIT
```

```

access-list TRANSIT; 3 elements

!-- Potential SNMP DoS (CSCse52679)

access-list TRANSIT line 1 extended deny udp any 192.168.131.0 255.255.255.0

!-- Potential HTTP DoS (CSCsf29974)

access-list TRANSIT line 2 extended deny tcp any 192.168.131.0 255.255.255.0

!-- Potentially FWSM Directed packet DoS(CSCse85707) or other unrelated traf.

access-list TRANSIT line 3 extended deny ip any 192.168.131.0 255.255.255.0

```

In the above example, two UDP/161, two TCP/443 and 490 IP packets have been dropped by the ACL configured on the outside interface.

Cisco IOS Switches



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

Mitigation: Access Control Lists (ACLs)

Access Control Lists ACLs (ACLs) can be used as effective mitigation for the FWSM directed packet processing DoS (Cisco Bug ID CSCse85707) and the HTTPS processing DoS (Cisco Bug ID CSCsf29974) vulnerabilities as well as provide an extra layer of protection for the malformed SNMP DoS (Cisco Bug ID CSCse52679). The following example, is for a core switch containing a FWSM module, therefore ACLs are device specific and placed outbound on the VLAN that the FWSM outside interface is a part of. Care should be taken to allow required traffic for routing or administrative access prior to denying all directed traffic. In the following example, the FWSM is at IP address 192.168.131.10.

```

!-- Permit additional Layer 3 and Layer 4 traffic destined for the FWSM
!-- address space as dictated by existing security policies and configuratio.

ip access-list extended FWSM-ACL

!-- Vulnerability-specific deny to aid identification SNMP DoS(CSCse52679)

deny udp any host 192.168.131.10 eq snmp

!-- Vulnerability-specific deny to aid identification HTTPS DoS(CSCsf29974)

deny tcp any host 192.168.131.10 eq 443

!-- Default deny to FWSM IP addresses
!-- Vulnerability-specific deny to aid identification FWSM Directed Packet
!--DoS(CSCse85707)

```

```
deny ip any host 192.168.131.10
```

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

```
!-- Vlan 131 is the Vlan the outside interface of the FWSM is in
```

```
interface vlan 131
ip access-group FWSM-ACL out
```

Identification: Access Control Lists (ACLs)

After the interface ACL is applied to the ingress interface, the command `show access-list acl-number` can be used to identify the number of packets being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit a vulnerability. The following is an example of output for the `show access-list FWSM-ACL` command.

```
#show access-lists FWSM-ACL
Extended IP access list FWSM-ACL

!-- Potential SNMP DoS (CSCse52679)

10 deny udp any host 192.168.131.10 eq snmp (2 matches)

!-- Potential HTTPS DoS (CSCsf29974)

20 deny tcp any host 192.168.131.10 eq 443

!-- Potential FWSM Directed Packet DoS (CSCse85707)

30 deny ip any host 192.168.131.10 (558 matches)
```

Identification: Netflow

NetFlow can be configured on switches to determine if attempts are in progress to exploit these vulnerabilities. Attempts to exploit the FWSM directed packet DoS (Cisco Bug ID CSCse85707) are likely to use protocols other than TCP, UDP, ICMP destined to infrastructure address space. Attempts to exploit the SNMP DoS (Cisco Bug ID CSCse52679) vulnerability are likely to show connections destined to infrastructure address space destined for port 161/UDP. Attempts to exploit the malformed HTTPS DoS (Cisco Bug ID CSCsf29974) are likely to show HTTPS connections directed to infrastructure address space. This first example has a high amount of *IP-Other* and *IPINIP* protocols which could be indicative of attempts to exploit the FWSM Directed Packet DoS.

```
router#show ip cache flow
MSFC:
IP packet size distribution (3907 total packets):
 1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  48
 .357 .636 .005 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .00
    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, 4456704 bytes
 91 active, 65445 inactive, 817 added
15991 aged polls, 0 flow alloc failures
Active flows timeout in 30 minutes
```

```

Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 270664 bytes
 91 active, 16293 inactive, 817 added, 817 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(Se |
|-----------------|------------|------------|----------|-----------|------------|-------------|-------------|
| ----- | Flows | /Sec | /Flow | /Pkt | /Sec | /Flow | /Flow |
| TCP-Telnet | 23 | 0.0 | 108 | 41 | 0.0 | 36.6 | 14.9 |
| UDP-NTP | 23 | 0.0 | 1 | 76 | 0.0 | 0.0 | 15.8 |
| UDP-other | 135 | 0.0 | 1 | 28 | 0.0 | 0.0 | 15.5 |
| ICMP | 2 | 0.0 | 2 | 28 | 0.0 | 1.0 | 15.3 |
| IGMP | 2 | 0.0 | 2 | 20 | 0.0 | 1.0 | 15.3 |
| IPINIP | 2 | 0.0 | 2 | 20 | 0.0 | 1.0 | 15.3 |
| GRE | 3 | 0.0 | 2 | 20 | 0.0 | 1.0 | 15.5 |
| IP-other | 536 | 0.0 | 2 | 20 | 0.0 | 1.0 | 15.3 |
| Total: | 726 | 0.0 | 5 | 34 | 0.0 | 1.9 | 15.4 |

The following example shows flows destined to port 161 (Hex 00A1):

```

router#show ip cache flow | include SrcIf| 00A1
SrcIf          SrcIPaddress  DstIf          DstIPaddress  Pr SrcP DstP  Pk
Vl1144        192.168.208.63 Null           192.168.131.10 11 88CB 00A1

```

Cisco Intrusion Prevention System



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

Identification: IPS Signatures

Cisco Intrusion Prevention System (IPS) can identify the vulnerabilities using the following signatures. Security personnel that monitor events should make sure these events are being monitored and that there is no potential for a false negative (alarm has been tuned too broadly). Links to the associated signatures are provided in the reference section at the end of the document.

Malformed SNMP DoS (Cisco Bug ID CSCse52679): Signature 4508 from Signature Update S43 which is enabled by default at a severity of informational. Security personnel should make sure they are monitoring for these events.

Malformed HTTP Request DoS (Cisco Bug ID CSCsd75794): Signature 5824/0 from Signature Update 271 will detect this vulnerability

Malformed SIP messages DoS (Cisco Bug ID CSCsg80915, CSCse27708, CSCsd97077): Signature 5825/0 from Signature Update 271 will detect this vulnerability

Malformed TCP packet DoS (Cisco Bug ID CSCsh12711): Signature 5837/0 from Signature Update 271 will detect this vulnerability.

Directed Packet Processing DoS (Cisco Bug ID CSCse85707): Signatures 1101, 1108, 1007, and 1109 provide partial detection. No one signature offers complete vulnerability coverage. The following protocols do not cause the vulnerability ICMP, IGMP, TCP, UDP, ESP, OSPF, PIM and Failover (IP Protocol numbers 1,2,6,17,50,89, and 105). IP Protocol numbers 11, 41, 53, 55, 77 and 134-255 can be detected with existing IPS signatures. Signature 1101 from signature pack 1, which

is enabled by default at a severity of *informational* covers IP protocols greater than 134. Signature 1108 from Signature Pack 27 which is enabled by default at severity level *high* will detect IP protocol 11 usage on the network. Signature 1007 from Signature Pack 118 which is a default severity of *informational* and disabled by default will detect IP Protocol 41 usage on the network. Signature 1109 subsigs 0 (IP Protocol 77), 1 (IP Protocol 55) and 2 (IP Protocol 53) is disabled by default and set to a severity of *medium*. For maximum identification capabilities security personnel should make sure signatures 1007, 1101, 1108, 1109/0, 1109/1 , 1109/2 and 1007 are enabled and set at a level high enough to alert security personnel. If these protocols are in use on the network, personnel may have to tune these events to their specific environment to avoid excessive false alarms. Custom IPS signatures could be created to augment the above mentioned signatures by covering the following IP protocol ranges 3-5, 7-10, 12-16, 18-40, 42-49, 51-52, 54, 56-76, 78-88, 90-104, and 106-133. Custom signature fidelity will depend on what protocols are actually used on the specific network. In some instances personnel may have to tune these events to their specific environment to avoid excessive false alarms. The following table summarizes the default status of the available signatures.

| Signature ID | Protocols Covered | Enabled Status | Alert Level |
|--------------|-------------------|----------------|---------------|
| 1007 | 41 | false | informational |
| 1101 | 134-255 | true | informational |
| 1108 | 11 | true | high |
| 1109 | 53,55,77 | false | medium |

Mitigation: IPS Signatures

To trigger preventative controls, the signatures will need to be configured to perform a response action. The actions that provide this type of mitigation are more effective when using an IPS device that is deployed in inline mode. With the exception of signature 5824/0 all of these events could potentially be spoofed, therefore the most prudent prevention measure is to produce an alert and drop the packet inline for events which could be spoofed. In the case of the FWSM Directed packet Processing DoS, administrators should make sure none of the protocols are legitimately being used. If other protocols are being used legitimately, the administrator, through tuning, could trigger response actions when only the FWSM devices are attack targets.

Cisco Security Monitoring, Analysis, and Response System

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) console can be monitored for attempts to exploit these vulnerabilities.

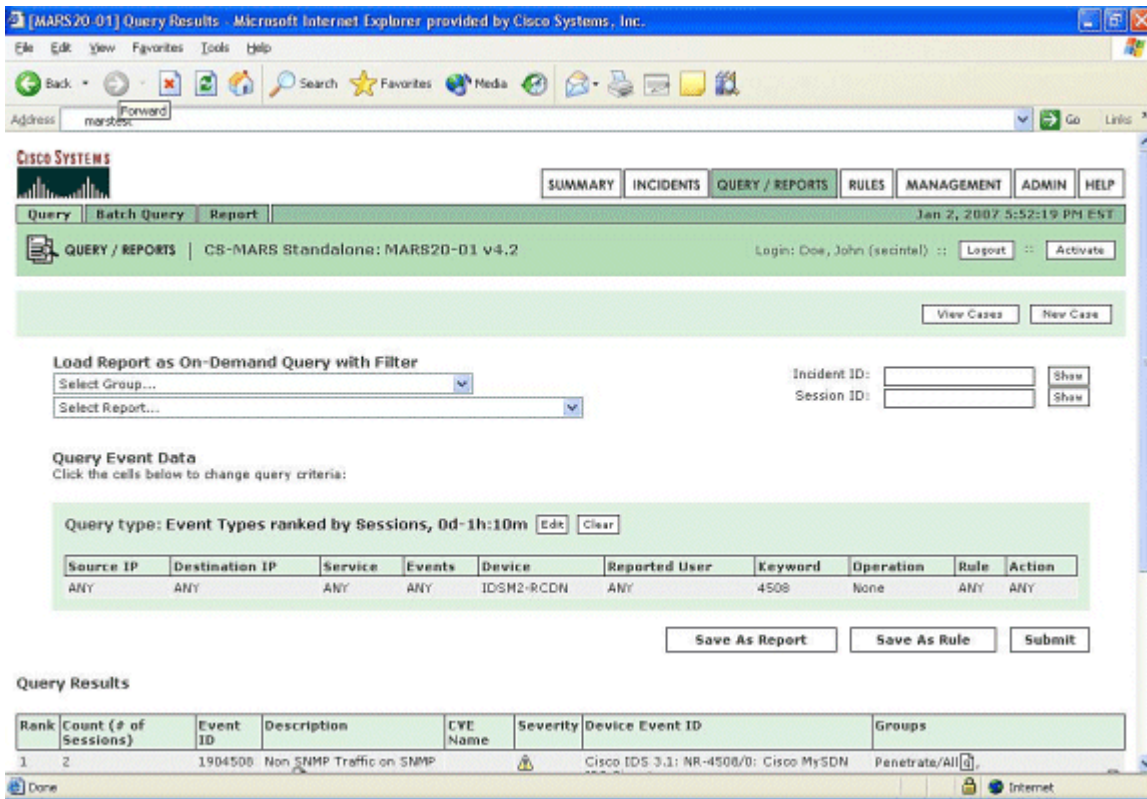
Identification: Directed packet processing DoS (Cisco Bug ID CSCse85707)

The following query will show events triggered by signatures that could be associated with attempts to exploit this vulnerability.

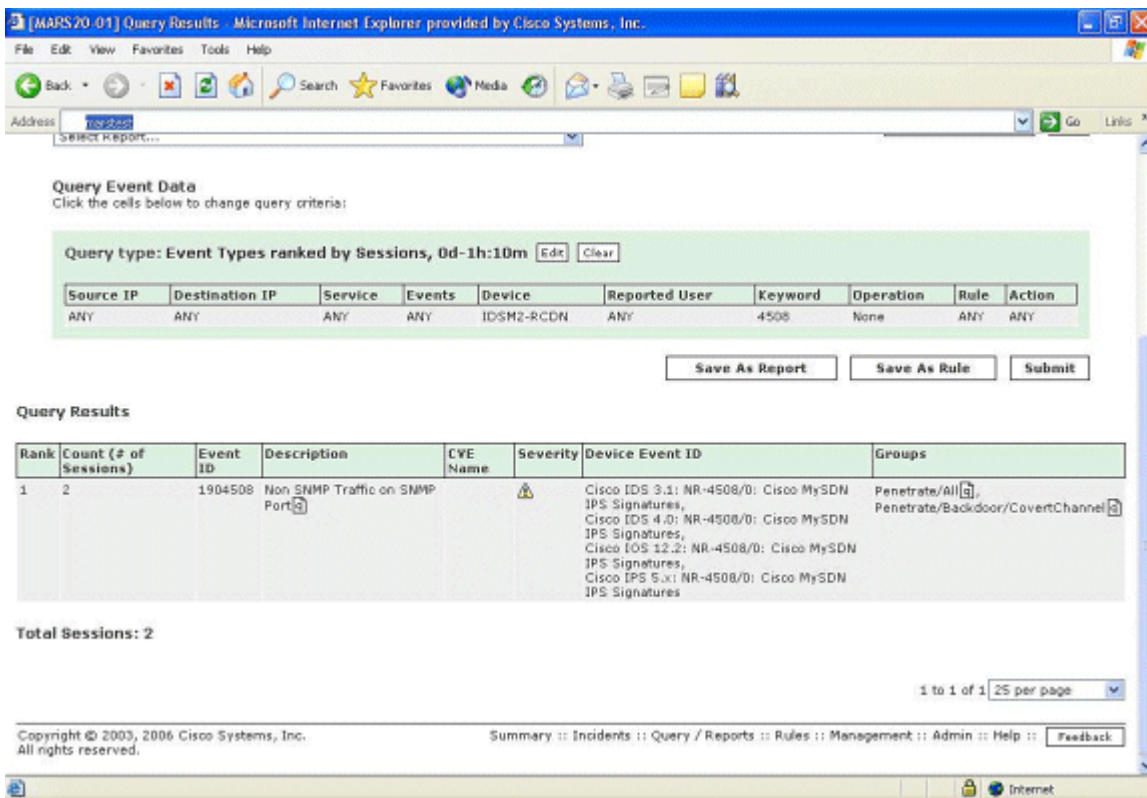
The display shown below is the result of the previous query.

Identification: Malformed SNMP request DoS vulnerability (Cisco Bug ID CS Cse52679)

The following query will show events triggered by signatures that could be associated with attempts to exploit this vulnerability.



The display shown below is the result of the previous query.



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-Feb-14 | 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

- **PSIRT Security Advisory:** <http://www.cisco.com/warp/public/707/cisco-sa-20070214-pix.shtml>
- **PSIRT Security Advisory:** <http://www.cisco.com/warp/public/707/cisco-sa-20070214-fwsm.shtml>
- [CISCO-IP-URPF-MIB Support](#)
- [Cisco Applied Mitigation Bulletins](#)
- [Cisco Guide to Harden Cisco IOS Devices](#)
- [Cisco Security Center](#)
- [Understanding Cross-Site Scripting \(XSS\) Threat Vectors](#)
- [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](#)
- [TTL Expiry Attack Identification and Mitigation](#)
- [A Security-Oriented Approach to IP Addressing](#)
- [Understanding Control Plane Protection](#)
- [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)

| | | | | | | |
|----------------------|----------------------------|-----------------------|-------------------------|--------------------------|--------------------------|----------------------|
| 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.](#)