

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the SIP Packets Reload IOS Devices with support for SIP Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20070131-sip.shtml>

## Revision 2.0

Last Updated 2007 February 9 2100 UTC (GMT)

For Public Release 2007 Jan 31 0900 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

The **SIP Packets Reload IOS Devices with support for SIP** vulnerability can be exploited remotely with no authentication and no user interaction. Successful exploitation may allow the attacker to cause a Denial of Service (DoS) condition. The attack vector is a specific series of packets destined to TCP port 5060 or UDP port 5060 on the affected device. This vulnerability is not covered by a CVE ID.

This document contains information to assist Cisco customers in mitigating attempts to exploit this vulnerability.

Vulnerable, non-affected and fixed software information is available in the PSIRT Security

Advisory:

<http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml>

## Mitigation Technique Overview

Cisco devices provide several countermeasures for the SIP Packets Reload IOS Devices with support for SIP vulnerability. The most preventive control is provided by disabling SIP as detailed in the security advisory. If SIP cannot be disabled, Control Plane Policing (CoPP) can be applied directly on affected devices as this will limit all attack vectors. Details on workarounds and mitigations that can be applied directly to the affected devices are in the PSIRT advisory at

<http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml>

Cisco IOS routers, Cisco PIX Security Appliances, Cisco ASA Adaptive Security Appliances, and Firewall Service Modules (FWSM) for Cisco Catalyst 6500 Switches and Cisco 7600 Routers, can provide effective preventive controls at the network level using access control lists (ACLs).

Detective controls can be performed through syslog messages and access control list show commands.

All of these features are detailed in the Device Specific Mitigation and Identification section below.

## Device-Specific Mitigation and Identification

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

- [Cisco IOS Router](#)
- [Cisco PIX/ASA/FWSM Firewalls](#)

### Cisco IOS Router



**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)

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 this 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 an 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 infrastrucur
!-- address space as dictated by existing security policies and configuratio.
!-- Permit/deny to infrastructure IP addresses in accordance with security p
!-- Vulnerability-specific denies to aid identification

access-list 150 deny tcp any 192.168.131.0 0.0.0.255 eq 5060
access-list 150 deny udp any 192.168.131.0 0.0.0.255 eq 5060

!-- Default deny to infrastructure IP addresses

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: Anti-Spoofing

This vulnerability can be exploited by spoofed packets. Anti-spoof protection in the form of Unicast Reverse Path Forwarding (uRPF) or interface access-lists can provide limited mitigation if properly configured. This mitigation should not be relied upon to provide 100% protection since spoofed packets may still enter the network from the interface expected by uRPF, be allowed by anti-spoofing access-lists, or appear to come from trusted source IP addresses. Also care must be taken to ensure that the appropriate uRPF mode (loose or strict) is configured so that legitimate packets are not dropped.

Additional information about Unicast Reverse Path Forwarding is available at: [Unicast Reverse Path Forwarding Loose Mode](#).

### 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 this vulnerability. The following is an example of output for the **show access-list 150** command configured inbound on interface gigabitEthernet 0/0.

```
Extended IP access list 150
 10 deny tcp any 192.168.131.0 0.0.0.255 eq 5060 (13 matches)
 20 deny udp any 192.168.131.0 0.0.0.255 eq 5060 (22 matches)
```

```
30 deny ip any 192.168.131.0 0.0.0.255
```

In the above example, 13 TCP/5060 and 22 UDP/5060 packets have been dropped by access-list 150. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability.

## Cisco PIX/ASA/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.

### Mitigation: Transit Access Control Lists (tACLs)

The following ACL is specifically designed to block attack traffic and should be deployed at the network edge as part of a transit access-list which will protect vulnerable routers behind it.

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.

Further information about transit ACLs is available in the white paper [Transit Access Control Lists: Filtering at Your Edge](#).

```
!-- Vulnerability-specific deny
```

```
access-list TRANSIT extended deny tcp any 192.168.131.0 255.255.255.0 eq 506  
access-list TRANSIT extended deny udp any 192.168.131.0 255.255.255.0 eq 506
```

```
!-- Network Infrastructure Deny
```

```
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: Transit Access Control Lists (tACLs)

After the transit 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. The following is an example of output for the **show access-list TRANSIT** command configured inbound on interface outside.

```
ASA#show access-list TRANSIT
access-list TRANSIT; 3 elements
access-list TRANSIT line 1 extended deny tcp any 192.168.131.0 255.255.255.0
access-list TRANSIT line 2 extended deny udp any 192.168.131.0 255.255.255.0
access-list TRANSIT line 3 extended deny ip any 192.168.131.0 255.255.255.0
```

In the above example, 26 TCP/5060 and 14 UDP/5060 packets have been dropped by access-list TRANSIT. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. In this instance, syslog message 106023 can provide additional context such as source IP address to aid in the investigation.

### Identification: Syslog Messages

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](#).

In the following example, the **show logging | grep message** command is used to see more details on denied entries. It is possible to modify the **grep** command in several ways to provide specific data (for instance, the name of the access list could be used instead or the word Deny). Viewing the specific logging entries, we see the source IP as 192.168.208.63 and a source port of 32886.

```
ASA#show logging | grep 106023
Jan 29 2007 12:09:25: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/5060 by access-group "TRANSIT" [0x298f38e5, 0x0]
Jan 29 2007 12:09:26: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/5060 by access-group "TRANSIT" [0x298f38e5, 0x0]
Jan 29 2007 12:09:28: %ASA-4-106023: Deny udp src outside:192.168.208.63/328
dst inside:192.168.131.10/5060 by access-group "TRANSIT" [0xce7a8141, 0x0]
Jan 29 2007 12:09:32: %ASA-4-106023: Deny udp src outside:192.168.208.63/328
dst inside:192.168.131.10/5060 by access-group "TRANSIT" [0xce7a8141, 0x0]
```

```
ASA#show logging | grep 192.168.208.63
Jan 29 2007 12:09:25: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/5060 by access-group "TRANSIT" [0x298f38e5, 0x0]
Jan 29 2007 12:09:26: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/5060 by access-group "TRANSIT" [0x298f38e5, 0x0]
Jan 29 2007 12:09:28: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/5060 by access-group "TRANSIT" [0x298f38e5, 0x0]
Jan 29 2007 12:09:32: %ASA-4-106023: Deny udp src outside:192.168.208.63/328
dst inside:192.168.131.10/5060 by access-group "TRANSIT" [0xce7a8141, 0x0]
Jan 29 2007 12:09:40: %ASA-4-106023: Deny udp src outside:192.168.208.63/328
dst inside:192.168.131.10/5060 by access-group "TRANSIT" [0xce7a8141, 0x0]
```

## 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 2.0	2007-February-09	Added uRPF.
Revision 1.0	2007-January-31	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

- [Cisco Network Foundation Protection \(NFP\) White Papers](#)
- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)

---

### 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.](#)