

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)

Applied Mitigation Bulletins

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

<http://www.cisco.com/warp/public/707/cisco-amb-20080326-dlsw.shtml>

## Revision 1.1

Last Updated 2008 August 19 1930 UTC (GMT)

For Public Release 2008 March 26 1600 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

## Contents

[Cisco Response](#)  
[Device Specific Mitigation and Identification](#)  
[Additional Information](#)  
[Revision History](#)  
[Cisco Security Procedures](#)  
[Related Information](#)

---

## Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisory *Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

### Vulnerability Characteristics

The Cisco IOS Software contains a vulnerability processing specially crafted Data-Link Switching (DLSw) packets. This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may result in a denial of service (DoS) condition. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition.

The attack vectors for exploitation are through packets using the following port and protocol:

- DLSw using UDP port 2067
- DLSw using IP protocol 91

An attacker could exploit this vulnerability using spoofed packets.

This vulnerability has been assigned CVE identifier CVE-2008-1152.

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-20080326-dlsw.shtml>.

## Mitigation Technique Overview

Cisco devices provide several countermeasures for the DLSw 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.

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 the vulnerabilities described in this document.

The proper deployment and configuration of Unicast RPF provides the most 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 the most effective means of protection against attacks with spoofed source MAC addresses.

Effective means of exploit prevention can also be provided by the Cisco ASA 5500 Series Adaptive Security Appliance, the Cisco PIX 500 Series Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers using the following:

- Transit Access Control Lists (tACLs)
- Unicast RPF

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

Effective use of Cisco Intrusion Prevention System (IPS) event actions provides visibility into and protection against attacks that attempt to exploit this vulnerability as discussed later in this document.

The proper deployment and configuration of Unicast RPF provides the most 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.

Cisco IOS NetFlow can provide visibility into these exploitation attempts using flow records.

Cisco IOS Software, Cisco ASA, 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 should 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 in Information Security Engagements](#) can help organizations develop repeatable security evaluation and response processes.

## Device Specific Mitigation and Identification



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

- [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

In an effort to protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators should 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.

In the following example, the address block 192.168.1.0/24 is the infrastructure address space and the host at 192.168.100.1 is considered a trusted endpoint. The iACL policy denies untrusted DLSw packets on UDP port 2067 and IP Protocol 91 sent to addresses that are part of the infrastructure address space. Care should be taken to allow required traffic for routing and administrative access prior to denying all traffic sent directly to infrastructure devices. 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 available in [Protecting Your Core: Infrastructure Protection](#)

## Access Control Lists.

```

ip access-list extended Infrastructure-ACL-Policy

!
!--- When applicable, include explicit permit statements for trusted
!--- sources that require access on the vulnerable port and protocol
!

permit udp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2067
permit 91 host 192.168.100.1 192.168.1.0 0.0.0.255

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

deny udp any 192.168.1.0 0.0.0.255 eq 2067
deny 91 any 192.168.1.0 0.0.0.255

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

deny ip any 192.168.1.0 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

!

```

## **Mitigation: Spoofing Protection**

### **Unicast Reverse Path Forwarding**

All 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 100 percent 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 should 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 available 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 available 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 DLSw packets on UDP port 2067 and IP protocol 91 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 192.168.100.1 192.168.1.0 0.0.0.255 eq 2067
 20 permit 91 host 192.168.100.1 192.168.1.0 0.0.0.255
 30 deny udp any 192.168.1.0 0.0.0.255 eq 2067 (31 matches)
 40 deny 91 any 192.168.1.0 0.0.0.255 (3 matches)
 50 deny ip any 192.168.1.0 0.0.0.255
router#
```

In the preceding example, the access list *Infrastructure-ACL-Policy* has dropped **31 DLSw** packets on **UDP** port **2067** for access control entry (ACE) sequence ID 30 and **3 DLSw** packets on **IP** protocol **91** for ACE sequence ID 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** or **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:** 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.

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.

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.

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 ip interface**, **show cef drop**, **show cef interface** *type slot/port internal*, 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 need to parse to view the desired information. Additional information about command modifiers is available in the "[show command](#)" sections of the Cisco IOS Configuration Fundamentals Command Reference.

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

```
router#show ip interface GigabitEthernet 0/0 | begin verify
--      CLI Output Truncated      --
      IP verify source reachable-via RX, allow default, allow self-ping
      18 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           18        0        0
IPv6 CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj
RP      0           0           0           3        0
router#

router#show cef interface GigabitEthernet 0/0 internal | include drop
--      CLI Output Truncated      --
      ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0, allow self-pin
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
        18 no route, 18 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 examples, Unicast RPF has dropped **18 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 Cisco Express Forwarding Forwarding Information Base.

## 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 the vulnerabilities described in this document. Administrators should investigate flows to determine whether they are attempts to exploit these vulnerabilities or whether they are legitimate traffic flows.

```

router#sh ip cache flow
IP packet size distribution (505 total packets):
  1-32  64  96  128  160  192  224  256  288  320  352  384  416  448  48
    .667 .332 .000 .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, 278544 bytes
  70 active, 4026 inactive, 70 added
  197 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 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
SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pk
Et0/0	192.168.152.37	Et0/1	192.168.251.82	11	343E	B392	
<b>Et0/0</b>	<b>192.168.247.249</b>	<b>Et0/1</b>	<b>192.168.1.242</b>	<b>11</b>	<b>9D61</b>	<b>0813</b>	
<b>Et0/0</b>	<b>192.168.77.108</b>	<b>Et0/1</b>	<b>192.168.1.125</b>	<b>5B</b>	<b>0000</b>	<b>0000</b>	
Et0/0	192.168.113.177	Et0/1	192.168.161.228	06	F100	B1D8	
Et0/0	192.168.105.207	Et0/1	192.168.142.166	06	74C3	7E5B	
<b>Et0/0</b>	<b>192.168.77.74</b>	<b>Et0/1</b>	<b>192.168.1.180</b>	<b>11</b>	<b>D2D5</b>	<b>0813</b>	
Et0/0	192.168.194.57	Et0/1	192.168.130.208	06	14DE	0B23	
<b>Et0/0</b>	<b>192.168.238.224</b>	<b>Et0/1</b>	<b>192.168.1.56</b>	<b>5B</b>	<b>0000</b>	<b>0000</b>	
Et0/0	192.168.158.234	Et0/1	192.168.224.187	11	9685	0FD3	
Et0/0	192.168.222.183	Et0/1	192.168.116.253	06	5D8A	27B6	
Et0/0	192.168.250.25	Et0/1	192.168.14.45	11	DE99	50B9	
<b>Et0/0</b>	<b>192.168.112.88</b>	<b>Et0/1</b>	<b>192.168.1.173</b>	<b>11</b>	<b>ED18</b>	<b>0813</b>	

```

Et0/0      192.168.105.65  Et0/1      192.168.113.241  11 1237 4E9E
Et0/0      192.168.191.120 Et0/1      192.168.7.220    06 82FD B289
Et0/0      192.168.224.144 Et0/1      192.168.141.8    11 E2AA 8792
Et0/0      192.168.158.190 Et0/1      192.168.87.107   06 38FC 0893
Et0/0      192.168.214.41  Et0/1      192.168.141.250  06 9982 9B7D
Et0/0      192.168.221.146 Et0/1      192.168.1.117    11 E533 0813
Et0/0      192.168.147.62  Et0/1      192.168.15.36    06 7E8A 995E
Et0/0      192.168.232.56  Et0/1      192.168.180.29   11 4DDB DB96
Et0/0      192.168.136.210 Et0/1      192.168.237.139  11 6BCA C7F5
Et0/0      192.168.121.156 Et0/1      192.168.7.5      06 B85E 9C8F
Et0/0      192.168.15.44   Et0/1      192.168.1.215    5B 0000 0000
Et0/0      192.168.50.19   Et0/1      192.168.132.67   06 257A 0FDB
router#

```

In the preceding example, there are multiple flows for **DLSw** on **UDP** port **2067** (hex value **0813**) and **IP** protocol **91** (hex value **5B**). Administrators should compare these flows to baseline utilization for DLSw traffic sent on UDP port 2067 and IP protocol 91 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

The command **show ip cache flow | include SrcIf|\_11\_.\*0813** will display only the traffic flows for packets using UDP port 2067 (hex value 0813), as shown here:

```

router#sh ip cache flow | include SrcIf|_11_.*0813
SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr  SrcP  DstP  Pk
Et0/0      192.168.224.74 Et0/1      192.168.1.234  11  EC58 0813
Et0/0      192.168.154.168 Et0/1      192.168.1.65   11  AAEB 0813
Et0/0      192.168.56.187  Et0/1      192.168.1.218  11  821B 0813
Et0/0      192.168.247.204 Et0/1      192.168.1.5    11  99A7 0813
Et0/0      192.168.40.228  Et0/1      192.168.1.153  11  90D2 0813
Et0/0      192.168.57.65   Et0/1      192.168.1.241  11  31B9 0813
Et0/0      192.168.197.164 Et0/1      192.168.1.112  11  B2ED 0813
Et0/0      192.168.204.123 Et0/1      192.168.1.10   11  68BF 0813
Et0/0      192.168.140.244 Et0/1      192.168.1.106  11  9926 0813
Et0/0      192.168.52.40   Et0/1      192.168.1.11   11  A47F 0813
Et0/0      192.168.124.93  Et0/1      192.168.1.40   11  2E94 0813
router#

```

The command **show ip cache flow | include SrcIf|\_5B\_** will display only the traffic flows for packets using IP protocol 91 (hex value 5B), as shown here:

```

router#sh ip cache flow | include SrcIf|_5B_
SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr  SrcP  DstP  Pk
Et0/0      192.168.29.18  Et0/1      192.168.1.134  5B  0000 0000
Et0/0      192.168.163.226 Et0/1      192.168.1.218  5B  0000 0000
Et0/0      192.168.248.187 Et0/1      192.168.1.83   5B  0000 0000
Et0/0      192.168.58.79  Et0/1      192.168.1.66   5B  0000 0000
Et0/0      192.168.68.125 Et0/1      192.168.1.115  5B  0000 0000
Et0/0      192.168.81.227 Et0/1      192.168.1.151  5B  0000 0000
Et0/0      192.168.38.68  Et0/1      192.168.1.178  5B  0000 0000
Et0/0      192.168.215.242 Et0/1      192.168.1.127  5B  0000 0000
Et0/0      192.168.0.63   Et0/1      192.168.1.93   5B  0000 0000
router#

```

## Cisco ASA, PIX, and FWSM Firewalls

### Mitigation: Transit Access Control Lists

In an effort 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 should 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.

The tACL policy denies unauthorized DLSw packets on UDP port 2067 and IP protocol 91 sent to affected devices. In the following example, 192.168.1.0/24 is the network IP address space 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 available in [Transit Access Control Lists: Filtering at Your Edge](#).

```

!
!--- Include any explicit permit statements for trusted sources
!--- that require access on the vulnerable port and protocol
!

access-list Transit-ACL-Policy extended permit udp host 192.168.100.1 192.16
access-list Transit-ACL-Policy extended permit 91 host 192.168.100.1 192.168

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

access-list Transit-ACL-Policy extended deny udp any 192.168.1.0 255.255.255
access-list Transit-ACL-Policy extended deny 91 any 192.168.1.0 255.255.255.

!
!--- 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 Transit-ACL-Policy extended deny ip any any

!
!--- Apply tACL to interfaces in the ingress direction
!

access-group Transit-ACL-Policy in interface outside

!

```

### Mitigation: Spoofing Protection Using Unicast Reverse Path Forwarding

All 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 100 percent 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 DLSw packets on UDP port 2067 and IP protocol 91 that have been filtered. Administrators should investigate filtered packets to determine whether they are attempts to exploit these vulnerabilities. Example output for **show access-list Transit-ACL-Policy** follows:

```
firewall#show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 5 elements
access-list Transit-ACL-Policy line 1 extended permit udp host 192.168.100.1
access-list Transit-ACL-Policy line 2 extended permit 91 host 192.168.100.1
access-list Transit-ACL-Policy line 3 extended deny udp any 192.168.1.0 255.
access-list Transit-ACL-Policy line 4 extended deny 91 any 192.168.1.0 255.2
access-list Transit-ACL-Policy line 5 extended deny ip any any (hitcnt=25)
firewall#
```

In the preceding example, the access list Transit-ACL-Policy has dropped **19 DLSw** packets on **UDP** port **2067** and **199 DLSw** packets using IP protocol **91** received from an untrusted host or network. In addition, syslog message *106023* can provide valuable information, which includes the source and destination IP address, the source and destination port numbers, and the IP protocol for the denied packet.

### 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 available 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 available in [Configuring Logging on the Cisco Security Appliance](#). Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available in [Configuring Monitoring and Logging on the Cisco FWSM](#).

In the following example, the **show logging | grep regex** command extracts syslog messages from the logging buffer on the firewall. These messages provide additional information about denied packets that could indicate attempts to exploit 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 available in [Using the Command Line Interface](#).

For additional information about investigating incidents using syslog events, reference the [Identifying Incidents Using Firewall and IOS Router Syslog Events](#) Applied Intelligence white paper.

```
firewall#show logging | grep 106023
Oct 10 2007 20:36:58: %ASA-4-106023: Deny udp src outside:192.168.143.24/595
inside:192.168.1.156/2067 by access-group "Transit-ACL-Policy"
Oct 10 2007 22:31:39: %ASA-4-106023: Deny protocol 91 src outside:192.168.20
```

```

inside:192.168.1.153 by access-group "Transit-ACL-Policy"
Oct 11 2007 22:39:12: %ASA-4-106023: Deny protocol 91 src outside:192.168.5.
inside:192.168.1.155 by access-group "Transit-ACL-Policy"
Oct 12 2007 08:33:35: %ASA-4-106023: Deny protocol 91 src outside:192.168.80
inside:192.168.1.204 by access-group "Transit-ACL-Policy"
Oct 12 2007 14:05:53: %ASA-4-106023: Deny udp src outside:192.168.85.153/684
inside:192.168.1.4/2067 by access-group "Transit-ACL-Policy"
Oct 13 2007 17:49:49: %ASA-4-106023: Deny udp src outside:192.168.81.231/133
inside:192.168.1.25/2067 by access-group "Transit-ACL-Policy"
firewall#

```

In the preceding example, the messages logged for the tACL *Transit-ACL-Policy* show potentially spoofed **DLSw** packets on **UDP** port **2067** and IP protocol **91** sent to the address block assigned to the network infrastructure.

Additional information about syslog messages for ASA and PIX security appliances is available in [Cisco Security Appliance System Log Messages](#). Additional information about syslog messages for the FWSM is available in [Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages](#).

### 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 available 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 available in [Configuring Logging on the Cisco Security Appliance](#). Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available in [Configuring Monitoring and Logging on the Cisco FWSM](#).

In the following example, the **show logging | grep regex** command extracts syslog messages from the logging buffer on the firewall. These messages provide additional information about denied packets that could indicate attempts to exploit 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 available in [Using the Command Line Interface](#).

```

firewall#show logging | grep 106021
Feb 21 2007 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
192.168.0.1 to 192.168.0.100 on interface outside
Feb 21 2007 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
192.168.0.1 to 192.168.0.100 on interface outside
Feb 21 2007 00:15:13: %ASA-1-106021: Deny TCP reverse path check from
192.168.0.1 to 192.168.0.100 on interface outside
firewall#

```

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

```

firewall#show asp drop

Frame drop:
Reverse-path verify failed

```

```

Flow is denied by configured rule          855
Expired flow                               1
Interface is down                          2

```

```
Flow drop:
```

```
firewall#
```

In the preceding example, Unicast RPF has dropped **11 IP packets** received on interfaces with Unicast RPF configured.

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 vulnerability described in this document. Starting with signature update S324 for sensors running Cisco IPS version 6.x or 5.x, the vulnerability described in this document can be detected by signature 6926/0 (Signature Name: Cisco IOS DLSw DoS). Signature 6926/0 is enabled by default, triggers a *Medium* severity event, has a signature fidelity rating (SFR) of 85, and is configured with a default event action of **produce-alert**. Signature 6926/0 fires when a single packet sent using UDP port 2067 is detected. Firing of this signature may indicate a potential exploit of the vulnerability described in this document.

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 described in this document.

Exploits that are easily spoofed 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 deployed in inline protection mode provides threat prevention against an attack that is attempting to exploit the vulnerability 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: 6926/0 - Cisco IOS DLSw DoS

```
ips#show events alert | include id=6926
```

```
evIdsAlert: eventId=1184140689302163325 severity=medium vendor=Cisco
originator:
  hostId: ips
  appName: sensorApp
  appInstanceId: 10952
time: 2008/03/26 18:45:30 2008/03/26 13:45:30 CDT
signature: description=Cisco IOS DLSw DoS id=6926 version=S324
  subsigId: 0
  sigDetails: Malformed DLSw UDP packet
  marsCategory: DoS/NetworkDevice
  marsCategory: Info/Misc
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 192.168.6.66
    port: 34188
  target:
    addr: locality=OUT 192.168.60.1
    port: 2067
    os: idSource=unknown relevance=unknown type=unknown
triggerPacket:
```

*!--- "triggerPacket" Output Truncated*

```
riskRatingValue: targetValueRating=medium 53
threatRatingValue: 53
interface: ge0_0
protocol: udp
```

ips#

## 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 on events for the multiple DLSw DoS vulnerabilities in Cisco IOS using IPS signature 6926/0 (Signature Name: Cisco IOS DLSw DoS). After the S324 dynamic signature update has been downloaded, using keyword **NR-6926/0** for IPS signature 6926/0 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 value used to query for event(s) created by the IPS signature related to this vulnerability:

The screenshot shows the Cisco MARS web interface. At the top, there are navigation tabs: SUMMARY, INCIDENTS, QUERY / REPORTS (selected), RULES, MANAGEMENT, ADMIN, and HELP. Below these are sub-tabs: Query, Batch Query, and Report. The main header area includes the text 'QUERY / REPORTS | CS-MARS Standalone: R4-MARS v4.3' and a login status 'Login: Administrator (padmin) :: Logout :: Activate'. A 'Select Case:' dropdown is set to 'No Case Selected...' with 'View Cases' and 'New Case' buttons.

The 'Query Event Data' section has a heading 'Query type: Event Raw Messages ranked by Time, 0h:10m' with 'Edit' and 'Clear' buttons. Below this is a table with columns: Source IP, Destination IP, Service, Events, Device, Reported User, Keyword, Operation, Rule, and Action. The data row shows: ANY, ANY, ANY, ANY, ANY, ANY, NR-6926/0, None, ANY, ANY. An 'Apply' button is to the right.

A modal window titled 'Specify raw message keywords:' is open. It has a table with columns: Open, Search String, Close, Operation, and Highlight. The first row is highlighted in red and contains: (, NR-6926/0, ), None, and a red highlight. Below this is a larger table with a red border around the first row, which has the same structure: Search String (NR-6926/0), Close, and Operation (None). Below this table are several empty rows for adding more keywords. 'Cancel' and 'Apply' buttons are at the bottom of the modal.

At the bottom of the page, there is a copyright notice: 'Copyright © 2003-2007 Cisco Systems, Inc. All rights reserved.' and a breadcrumb trail: 'Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help'.

The following screen shot shows the query results for this vulnerability created by the Cisco Security MARS appliance:

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. MARS will not include these events in inspection rules, thus 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 and instructions for configuring dynamic signature updates are available for the Cisco Security MARS [4.3.1](#) and [5.3.1](#) releases.

## Additional Information

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

## Revision History


Revision 1.1	2008- August- 19	Corrected link in Identification: Spoofing Protection Using Unicast Reverse Path Forwarding section
Revision 1.0	2008- March-26	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 Applied Mitigation Bulletin Documents](#)
- [Cisco Security Center](#)
- [Identifying Incidents Using Firewall and IOS Router Syslog Events](#)
- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
- [A Security-Oriented Approach to IP Addressing](#)
- [Cisco 6.x Intrusion Prevention System](#)
- [Cisco IPS 6.x Signature Downloads](#) ( [registered customers only](#) )
- [Cisco IPS Signature Search Page](#)
- [Risk Rating and Threat Rating: Simplify IPS Policy Management](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Understanding Access Control List Logging](#)
- [Understanding Unicast Reverse Path Forwarding](#)
- [Cisco IOS NetFlow White Papers](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco Network Foundation Protection Presentations](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Unicast Reverse Path Forwarding Loose Mode](#)
- [Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider - Internet Service Provider Network Edge](#)
- [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)

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

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

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