

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

Security Advisories

# Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

Advisory ID: cisco-sa-20080326-dlsw

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

## Revision 1.5

Last Updated 2008 June 26 2400 UTC (GMT)

For Public Release 2008 March 26 1600 UTC (GMT)

---

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

---

## Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Vulnerability Scoring Details](#)
- [Impact](#)
- [Software Versions and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of this Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

---

## Summary

Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml>.

**Note:** The March 26, 2008 publication includes five Security Advisories. The Advisories all affect Cisco's Internetwork Operating System (IOS). Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities in all five Advisories.

**Individual publication links are listed below:**

- Cisco IOS Virtual Private Dial-up Network Denial of Service Vulnerability  
<http://www.cisco.com/warp/public/707/cisco-sa-20080326-pptp.shtml>
- Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS  
<http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml>
- Cisco IOS User Datagram Protocol Delivery Issue For IPv4/IPv6 Dual-stack Routers  
<http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml>
- Vulnerability in Cisco IOS with OSPF, MPLS VPN, and Supervisor 32, Supervisor 720, or Route Switch Processor 720  
<http://www.cisco.com/warp/public/707/cisco-sa-20080326-queue.shtml>
- Cisco IOS Multicast Virtual Private Network (MVPN) Data Leak  
<http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml>

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

## ☐ Affected Products

### ☐ Vulnerable Products

This security advisory applies to all Cisco products that run any version of affected Cisco IOS software configured for DLSw. Systems that contain the DLSw feature, but do not have it enabled, are not affected.

Routers enabled for DLSw contain a line in the configuration defining a local DLSw peer. This configuration can be observed by issuing the command **show running-config**. Systems configured for DLSw contain lines similar to the following:

```
dlsw local-peer
```

or

```
dlsw local-peer peer-id <IP address>
```

Any version of Cisco IOS prior to the versions which are listed in the Software Versions and Fixes section below is vulnerable.

To determine the version of Cisco IOS software running on a Cisco product, log in to the device and issue the **show version** command to display the system banner. Cisco IOS Software will identify itself as "Internetwork Operating System Software" or simply "IOS". On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the show version command or will give different output.

The following example identifies a Cisco product running Cisco IOS Software Release 12.3(6) with an installed image name of C3640-IS-M:

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-IS-M), Version 12.3(6), RELEASE SOFTWARE
```

The next example shows a product running Cisco IOS Software Release 12.3(11)T3 with an image name of C3845-ADVIPSERVICESK9-M:

```
Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 1
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
```

Additional information about Cisco IOS release naming can be found at <http://www.cisco.com/warp/public/620/1.html>.

## ☐ Products Confirmed Not Vulnerable

Cisco IOS devices that are not configured for DLSw are not vulnerable.

No other Cisco products are currently known to be affected by these vulnerabilities.

[Top of the section](#)   [Close Section](#)

## ☐ Details

Data-link switching (DLSw) provides a means of transporting IBM Systems Network Architecture (SNA) and network basic input/output system (NetBIOS) traffic over an IP network. Cisco implementation of DLSw also uses UDP port 2067 and IP Protocol 91 for Fast Sequenced Transport (FST).

Multiple vulnerabilities exist in Cisco IOS when processing UDP and IP protocol 91 packets. These vulnerabilities do not affect TCP packet processing. A successful exploitation may result in a reload of the system or a memory leak on the device, leading to a denial of service (DoS) condition.

Cisco IOS devices configured for DLSw with **dlsw local-peer** automatically listen for IP protocol 91 packets. A Cisco IOS device that is configured for DLSw with the **dlsw local-peer peer-id <IP-address>** command listens for IP protocol 91 packets and UDP port 2067.

Cisco IOS devices listen to IP protocol 91 packets when DLSw is configured. However, it is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

```
dlsw remote-peer 0 fst <ip-address>
```

It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets, it does not prevent the device from receiving and processing incoming UDP packets.

These vulnerabilities are documented in Cisco Bug ID [CSCsk73104](#) ([registered](#) customers only) and have been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2008-1152.

[Top of the section](#)   [Close Section](#)

## ▣ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

CSCsk73104 - Handling of malformed packets by DLSW					
Calculate the environmental score of <a href="#">CSCsk73104</a>					
CVSS Base Score - <b>7.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - <b>6.4</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

[Top of the section](#)   [Close Section](#)

## ▣ Impact

Successful exploitation of these vulnerabilities may result in the reload of the device or memory leaks, leading to a DoS condition.

[Top of the section](#)   [Close Section](#)

## ▣ Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be

supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Each row of the Cisco IOS software table (below) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

<b>Major Release</b>	<b>Availability of Repaired Releases</b>	
<b>Affected 12.0-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.0	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.0DA	Releases prior to 12.0(8)DA3 are vulnerable, release 12.0(8)DA3 and later are not vulnerable; migrate to any release in 12.2DA	
12.0DB	Releases prior to 12.0(7)DB are vulnerable, release 12.0(7)DB and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.0DC	Releases prior to 12.0(7)DC are vulnerable, release 12.0(7)DC and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.0S	Releases prior to 12.0(17)S5 are vulnerable, release 12.0(17)S5 and later are not vulnerable;	
12.0SC	Not Vulnerable	
12.0SL	Not Vulnerable	
12.0SP	Not Vulnerable	
12.0ST	Not Vulnerable	
12.0SX	Not Vulnerable	
12.0SY	Not Vulnerable	

12.0SZ	Not Vulnerable	
12.0T	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.0W	Vulnerable; contact TAC	12.0(3c)W5(8)
12.0WC	Vulnerable; contact TAC	
12.0WT	Not Vulnerable	
12.0XA	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.0XB	Not Vulnerable	
12.0XC	Releases prior to 12.0(2)XC2 are vulnerable, release 12.0(2)XC2 and later are not vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.0XD	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.0XE	Vulnerable; first fixed in <a href="#">12.1E</a>	
12.0XF	Not Vulnerable	
12.0XG	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.0XH	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.0XI	Releases prior to 12.0(4)XI2 are vulnerable, release 12.0(4)XI2 and later are not vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.0XJ	Releases prior to 12.0(4)XJ5 are vulnerable, release 12.0(4)XJ5 and later are not vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.0XK	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.0XL	Not Vulnerable	
12.0XM	Not Vulnerable	
12.0XN	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)

12.0XQ	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.0XR	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.0XS	Not Vulnerable	
12.0XV	Not Vulnerable	
12.0XW	Not Vulnerable	
<b>Affected 12.1-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.1	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1AA	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1AX	Not Vulnerable	
12.1AY	Releases prior to 12.1(22)AY1 are vulnerable, release 12.1(22)AY1 and later are not vulnerable;	12.1(22)EA11
12.1AZ	Not Vulnerable	
12.1CX	Not Vulnerable	
12.1DA	Not Vulnerable	
12.1DB	Releases prior to 12.1(4)DB1 are vulnerable, release 12.1(4)DB1 and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.1DC	Releases prior to 12.1(4)DC2 are vulnerable, release 12.1(4)DC2 and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.1E	12.1(27b)E4	
12.1EA	Releases prior to 12.1(11)EA1 are vulnerable, release 12.1(11)EA1 and later are not vulnerable;	12.1(22)EA11
12.1EB	Not Vulnerable	
12.1EC	Vulnerable; migrate to any release in 12.2BC	12.3(23)BC1

12.1EO	Not Vulnerable	
12.1EU	Not Vulnerable	
12.1EV	Not Vulnerable	
12.1EW	Not Vulnerable	
12.1EX	Vulnerable; first fixed in <a href="#">12.1E</a>	
12.1EY	Not Vulnerable	
12.1EZ	Vulnerable; first fixed in <a href="#">12.1E</a>	
12.1GA	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1GB	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1T	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XA	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XB	Not Vulnerable	
12.1XC	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XD	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XE	Not Vulnerable	
12.1XF	Not Vulnerable	
12.1XG	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XH	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XI	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XJ	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XK	Not Vulnerable	
12.1XL	Not Vulnerable	
12.1XM	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XN	Not Vulnerable	
12.1XO	Not Vulnerable	
12.1XP	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
	Vulnerable; first fixed	

12.1XQ	in <a href="#">12.3</a>	12.3(26)
12.1XR	Not Vulnerable	
12.1XS	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XT	Releases prior to 12.1(3)XT2 are vulnerable, release 12.1(3)XT2 and later are not vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XU	Not Vulnerable	
12.1XV	Releases prior to 12.1(5)XV1 are vulnerable, release 12.1(5)XV1 and later are not vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XW	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XX	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XY	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1XZ	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1YA	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1YB	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1YC	Not Vulnerable	
12.1YD	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1YE	Releases prior to 12.1(5)YE1 are vulnerable, release 12.1(5)YE1 and later are not vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1YF	Not Vulnerable	
12.1YG	Not Vulnerable	
12.1YH	Not Vulnerable	
12.1YI	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.1YJ	Not Vulnerable	

<b>Affected 12.2-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.2	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2B	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2BC	Not Vulnerable	
12.2BW	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2BY	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2BZ	Not Vulnerable	
12.2CX	Not Vulnerable	
12.2CY	Not Vulnerable	
12.2CZ	Not Vulnerable	
12.2DA	Not Vulnerable	
12.2DD	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2DX	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2EU	Not Vulnerable	
12.2EW	Not Vulnerable	
12.2EWA	Not Vulnerable	
12.2EX	Releases prior to 12.2(20)EX are vulnerable, release 12.2(20)EX and later are not vulnerable; migrate to any release in 12.2SEA	12.2(40)EX1
12.2EY	Not Vulnerable	
12.2EZ	Not Vulnerable	
12.2FX	Not Vulnerable	
12.2FY	Not Vulnerable	
12.2FZ	Not Vulnerable	
12.2IXA	Vulnerable; contact TAC	
12.2IXB	Vulnerable; contact TAC	
12.2IXC	Vulnerable; contact TAC	

12.2IXD	Vulnerable; contact TAC	
12.2IXE	Vulnerable; migrate to any release in 12.2IXF	12.2(18)IXF; Available on 31-MAR-08
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	12.2(15)MC2h	12.2(15)MC2k
12.2S	12.2(25)S15	12.2(25)S15
12.2SB	12.2(28)SB10 12.2(31)SB9 12.2(33)SB; Available on 31-MAR-2008	12.2(31)SB11
12.2SBC	Vulnerable; first fixed in <a href="#">12.2SB</a> ; Available on 31-MAR-2008	12.2(31)SB11
12.2SCA	Not Vulnerable	
12.2SE	Not Vulnerable	
12.2SEA	Not Vulnerable	
12.2SEB	Not Vulnerable	
12.2SEC	Not Vulnerable	
12.2SED	Not Vulnerable	
12.2SEE	Not Vulnerable	
12.2SEF	Not Vulnerable	
12.2SEG	Not Vulnerable	
12.2SG	12.2(44)SG	12.2(44)SG
12.2SGA	Not Vulnerable	
12.2SL	Not Vulnerable	
12.2SM	Not Vulnerable	
12.2SO	Not Vulnerable	
12.2SRA	12.2(33)SRA6	12.2(33)SRA7
12.2SRB	12.2(33)SRB3; Available on 07-APR-2008	12.2(33)SRB3; Available on 14-APR-08
12.2SRC	Not Vulnerable	
12.2SU	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)

12.2SV	Releases prior to 12.2(29a)SV1 are vulnerable, release 12.2(29a)SV1 and later are not vulnerable; migrate to any release in 12.2SVA	12.2(29b)SV
12.2SVA	Not Vulnerable	
12.2SVC	Not Vulnerable	
12.2SVD	Not Vulnerable	
12.2SW	Releases prior to 12.2(25)SW10 are vulnerable, release 12.2(25)SW10 and later are not vulnerable;	
12.2SX	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF13
12.2SXA	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF13
12.2SXB	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF13
12.2SXD	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF13
12.2SXE	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF13
12.2SXF	12.2(18)SXF12 12.2(18)SXF12a	12.2(18)SXF13
12.2SXH	12.2(33)SXH1	12.2(33)SXH2
12.2SY	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF13
12.2SZ	Vulnerable; first fixed in <a href="#">12.2S</a>	12.2(25)S15 12.2(31)SB11 12.2(33)SRC
12.2T	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2TPC	12.2(8)TPC10d	
12.2UZ	Not Vulnerable	
12.2XA	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2XB	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)

12.2XC	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2XD	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2XE	Not Vulnerable	
12.2XF	Not Vulnerable	
12.2XG	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2XH	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2XI	Not Vulnerable	
12.2XJ	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2XK	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2XL	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2XM	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2XN	12.2(33)XN1	12.3(26)
12.2XO	Not Vulnerable	
12.2XQ	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2XR	Not Vulnerable	
12.2XS	Not Vulnerable	
12.2XT	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2XU	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2XV	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2XW	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2YA	Releases prior to 12.2(4)YA8 are vulnerable, release 12.2(4)YA8 and later are not vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2YB	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2YC	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)

12.2YD	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2YE	Vulnerable; first fixed in <a href="#">12.2S</a>	12.2(25)S15 12.2(31)SB11 12.2(33)SRC
12.2YF	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2YG	Not Vulnerable	
12.2YH	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2YJ	Releases prior to 12.2(8)YJ1 are vulnerable, release 12.2(8)YJ1 and later are not vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2YK	Not Vulnerable	
12.2YL	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2YM	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2YN	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2YO	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF13
12.2YP	Not Vulnerable	
12.2YQ	Not Vulnerable	
12.2YR	Not Vulnerable	
12.2YS	Not Vulnerable	
12.2YT	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2YU	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2YV	Releases prior to 12.2(11)YV1 are vulnerable, release 12.2(11)YV1 and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2YW	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2YX	Vulnerable; first fixed	12.4(18a)

	in <a href="#">12.4</a>	
12.2YY	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2YZ	Vulnerable; first fixed in <a href="#">12.2S</a>	12.2(25)S15 12.2(31)SB11 12.2(33)SRC
12.2ZA	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF13
12.2ZB	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2ZC	Not Vulnerable	
12.2ZD	Vulnerable; contact TAC	
12.2ZE	Vulnerable; first fixed in <a href="#">12.3</a>	12.3(26)
12.2ZF	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2ZG	Not Vulnerable	
12.2ZH	Releases prior to 12.2(13)ZH6 are vulnerable, release 12.2(13)ZH6 and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.2(13)ZH11
12.2ZJ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.2ZL	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T4 12.4(18a)
12.2ZP	Not Vulnerable	
12.2ZU	Vulnerable; first fixed in <a href="#">12.2SXH</a>	12.2(33)SXH2
12.2ZY	12.2(18)ZY2	12.2(18)ZY2
<b>Affected 12.3-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.3	12.3(24)	12.3(26)
12.3B	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.3BC	Not Vulnerable	
12.3BW	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)

12.3EU	Not Vulnerable	
12.3JA	Not Vulnerable	
12.3JEA	Not Vulnerable	
12.3JEB	Not Vulnerable	
12.3JEC	Not Vulnerable	
12.3JK	Releases prior to 12.3(8)JK1 are vulnerable, release 12.3(8)JK1 and later are not vulnerable;	12.3(8)JK1
12.3JL	Not Vulnerable	
12.3JX	Not Vulnerable	
12.3T	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.3TPC	Not Vulnerable	
12.3VA	Vulnerable; contact TAC	
12.3XA	12.3(2)XA7; Available on 31-MAR-2008	12.3(2)XA7; Available on 31-MAR-08
12.3XB	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.3XC	12.3(2)XC5	12.4(15)T4 12.4(18a)
12.3XD	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.3XE	12.3(2)XE6; Available on 31-MAR-2008	12.4(15)T4 12.4(18a)
12.3XF	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.3XG	Vulnerable; first fixed in <a href="#">12.3YG</a> ; Available on 16-JUN-2008	12.4(15)T4 12.4(18a)
12.3XH	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.3XI	12.3(7)XI11; Available on 18-SEP-2008	
12.3XJ	Vulnerable; first fixed in <a href="#">12.3YX</a>	12.3(14)YX11 12.4(15)T4
12.3XK	Vulnerable; first fixed	12.4(18a)

	in <a href="#">12.4</a>	
12.3XQ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18a)
12.3XR	12.3(7)XR8; Available on 31-MAR-2008	12.3(7)XR8; Available on 31-MAR-08
12.3XS	Not Vulnerable	
12.3XU	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T4
12.3XW	Vulnerable; first fixed in <a href="#">12.3YX</a>	12.3(14)YX11 12.4(15)T4
12.3XY	Not Vulnerable	
12.3YA	Not Vulnerable	
12.3YD	Not Vulnerable	
12.3YF	Vulnerable; first fixed in <a href="#">12.3YX</a>	12.3(14)YX11 12.4(15)T4
12.3YG	12.3(8)YG7; Available on 16-JUN-2008	12.4(15)T4
12.3YH	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T4
12.3YI	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T4
12.3YJ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T4
12.3YK	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T4
12.3YM	12.3(14)YM12	12.3(14)YM12
12.3YQ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T4
12.3YS	12.3(11)YS3; Available on 31-MAR-2008	12.4(15)T4
12.3YT	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T4
12.3YU	Vulnerable; first fixed in <a href="#">12.4XB</a>	
12.3YX	12.3(14)YX11	12.3(14)YX11
12.3YZ	12.3(11)YZ3	
<b>Affected 12.4-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>

12.4	12.4(10c) 12.4(13e) 12.4(16b) 12.4(17) 12.4(3h) 12.4(8d)	12.4(18a)
12.4JA	Not Vulnerable	
12.4JK	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JMC	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MR	Not Vulnerable	
12.4SW	Vulnerable; contact TAC	12.4(15)SW
12.4T	12.4(15)T2 12.4(6)T10 12.4(9)T7	12.4(15)T4
12.4XA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T4
12.4XB	12.4(2)XB6	
12.4XC	Vulnerable; contact TAC	
12.4XD	12.4(4)XD10	12.4(4)XD10
12.4XE	12.4(6)XE2	12.4(15)T4
12.4XF	Not Vulnerable	
12.4XG	12.4(9)XG2	12.4(9)XG2
12.4XJ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T4
12.4XK	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T4
12.4XL	12.4(15)XL2	12.4(15)XL2
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	

12.4XT	12.4(6)XT2	12.4(6)XT2
12.4XV	12.4(11)XV	
12.4XW	Vulnerable; contact TAC	12.4(11)XW6
12.4XY	Not Vulnerable	

A special patch for Cisco IOS Software Modularity is also available for 12.2(18)SXF11 and can be downloaded from the Cisco IOS Software Modularity Patch Navigator at [http://tools.cisco.com/swdf/ionpn/jsp/result.jsp?s\\_tarballWild=mp001-p.122-18.SXF11&reqType=cWork](http://tools.cisco.com/swdf/ionpn/jsp/result.jsp?s_tarballWild=mp001-p.122-18.SXF11&reqType=cWork).

[Top of the section](#)   [Close Section](#)

## Workarounds

The workaround consists of filtering UDP packets to port 2067 and IP protocol 91 packets. Filters can be applied at network boundaries to filter all IP protocol 91 packets and UDP packets to port 2067 or can be applied on individual affected devices to permit such traffic only from trusted peer IP addresses. However, since both of the protocols are connectionless, it is possible for an attacker to spoof malformed packets from legitimate peer IP addresses.

As soon as DLSw is configured, the Cisco IOS device begins listening on IP protocol 91. However, this protocol is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

```
dlsw remote-peer 0 fst <ip-address>
```

If FST is used, filtering IP protocol 91 will break the operation, so filters need to permit protocol 91 traffic from legitimate peer IP addresses.

It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets, it does not prevent the receiving and processing of incoming UDP packets. To protect a vulnerable device from malicious packets via UDP port 2067, both of the following actions must be taken:

1. Disable UDP outgoing packets with the "dlsw udp-disable" command, AND
2. Filter UDP 2067 in the vulnerable device using infrastructure ACL.

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

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

### Using Control Plane Policing on Affected Devices

Control Plane Policing (CoPP) can be used to block untrusted DLSw traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example, which uses 192.168.100.1 to represent a trusted host, can

be adapted to your network. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```

!--- Deny DLSw traffic from trusted hosts to all IP addresses
!--- configured on all interfaces of the affected device so that
!--- it will be allowed by the CoPP feature

access-list 111 deny udp host 192.168.100.1 any eq 2067
access-list 111 deny 91 host 192.168.100.1 any

!--- Permit all other DLSw traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so that it
!--- will be policed and dropped by the CoPP feature

access-list 111 permit udp any any eq 2067
access-list 111 permit 91 any any

!--- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and Layer 4
!--- traffic in accordance with existing security policies and
!--- configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all drop-DLSw-class
  match access-group 111

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-DLSw-traffic
  class drop-DLSw-class
    drop

!--- Apply the Policy-Map to the Control-Plane of the
!--- device

control-plane
  service-policy input drop-DLSw-traffic

```

In the above CoPP example, the access control entries (ACEs) which match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Please note that in the Cisco IOS 12.2S and 12.0S trains the policy-map syntax is different:

```

policy-map drop-DLSw-traffic
  class drop-DLSw-class
    police 32000 1500 1500 conform-action drop exceed-action drop

```

Additional information on the configuration and use of the CoPP feature is available at

[http://www.cisco.com/en/US/products/ps6642/products\\_white\\_paper0900aecd804fa16a.shtml](http://www.cisco.com/en/US/products/ps6642/products_white_paper0900aecd804fa16a.shtml)

and

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products\\_feature\\_guide09186a008052](http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a008052)

## Using Infrastructure ACLs at Network Boundary

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. iACLs are 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 iACL example shown below should be included as part of the deployed infrastructure access-list that will protect all devices with IP addresses in the infrastructure IP address range. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```

!--- Permit DLSw (UDP port 2067 and IP protocol 91) packets
!--- from trusted hosts destined to infrastructure addresses.

access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MA
access-list 150 permit 91 TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MAS

!--- Deny DLSw (UDP port 2067 and IP protocol 91) packets from
!--- all other sources destined to infrastructure addresses.

access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 2067
access-list 150 deny 91 any INFRASTRUCTURE_ADDRESSES MASK

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

access-list 150 permit ip any any

interface serial 2/0
 ip access-group 150 in

```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_white\\_paper09186a00801a1a55.shtr](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtr)

[Top of the section](#)   [Close Section](#)

## ☐ Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at [http://www.cisco.com/en/US/products/prod\\_warranties\\_item09186a008088e31f.html](http://www.cisco.com/en/US/products/prod_warranties_item09186a008088e31f.html), or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact [psirt@cisco.com](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto:security-alert@cisco.com) for software upgrades.

### ☐ **Customers with Service Contracts**

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

### ☐ **Customers using Third Party Support Organizations**

Customers whose Cisco products are provided or maintained through prior or existing agreements with third-party support organizations, such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations, such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

### ☐ **Customers without Service Contracts**

Customers who purchase direct from Cisco but do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: [tac@cisco.com](mailto:tac@cisco.com)

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#)   [Close Section](#)

## ☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability

described in this advisory.

These vulnerabilities were found internally.

[Top of the section](#)   [Close Section](#)

## ☐ Status of this Notice: FINAL

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.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

[Top of the section](#)   [Close Section](#)

## ☐ Distribution

This advisory is posted on Cisco's worldwide website at :

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

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto:comp.dcom.sys.cisco@newsgate.cisco.com)

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

[Top of the section](#)   [Close Section](#)

## ☐ Revision History

Revision 1.5	2008- June- 26	Updated Summary to remove link and verbiage.
	2008-	

Revision 1.4	April-25	Updated link to the CVSS score of <a href="#">CSCsk73104</a> .
Revision 1.3	2008-Apr-21	Added the specific link for IOS Software Modularity patch
Revision 1.2	2008-Mar-31	Replacing IOS First Fixed Table with correct table -- data visible between 3/28 and 3/31 was incorrect
Revision 1.1	2008-Mar-29	Updated Software Table for 12.0S, 12.0SY, 12.0SX and 12.0SZ due to new information on advisory ID <a href="#">cisco-sa-20080326-IPv4IPv6</a> , the March 26th advisory on IPv4IPv6 Dual Stack Routers.
Revision 1.0	2008-Mar-26	Initial public release

[Top of the section](#)   [Close Section](#)

## ☐ 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>.

[Top of the section](#)   [Close Section](#)

---

<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.](#)