

Cisco Security Advisory: DLSw Vulnerability

Advisory ID: cisco-sa-20070110-dlsw

<http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml>

Revision 1.2

Last Updated 2007 April 20 2325 UTC (GMT)

For Public Release 2007 January 10 1600 UTC (GMT)

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

Contents

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

Summary

A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

There are workarounds available for this vulnerability, as detailed in the [Workarounds](#) section below.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml>

☐ Affected Products

☐ Vulnerable Products

This security advisory applies to all Cisco products that run Cisco IOS Software versions 11.0 through 12.4 configured for DLSw. A system which contains the DLSw feature, but does not have it enabled, is not affected.

A router which is configured for DLSw will have a line in the configurations defining a local DLSw peer. This definition can be seen by issuing the command **show running-config** and looking for lines similar to the following:

```
dlsw local-peer peer-id
```

To determine if DLSw is enabled on your Cisco IOS device, it is also possible to issue the **show dlsw statistics** command while in enable mode and look for output similar to:

```
Router#show dlsw statistics
DLSw+ Control Queue Statistics:
  SNA Control Queue (count/max/dropped):      (0/0/0)
  Netbios Control Queue (count/max/dropped):  (0/0/0)
  Other Control Queue (count/max/dropped):    (0/100/0)
  Critical Control Queue (count/max):         (0/0)

DLSw+ Border Peer Caching Statistics:

  0 Border Peer Frames processed
  0 Border frames found Local
  0 Border frames found Remote
  0 Border frames found Group Cache
```

A device which is not configured for DLSw will simply return to a command prompt with no output.

A device which does not support the DLSw feature will return output similar to:

```
Router#show dlsw statistics
      ^
% Invalid input detected at '^' marker.
```

Any version of Cisco IOS prior to the versions which will be listed in the [Software Versions and Fixes](#) section below may be 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 IOS release 12.3(6) with an installed image name of C3640-I-M:

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

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

```
Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.3
RELEASE SOFTWARE (fc4)
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>.

No other Cisco products are currently known to be affected by the vulnerability addressed in this advisory.

▣ Products Confirmed Not Vulnerable

Products confirmed not to be vulnerable include devices which are not configured for DLSw.

[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.

Establishing DLSw communications involves several operational stages.

1. In phase one, DLSw peers establish two TCP connections with each other via TCP ports 2065 or 2067. Those TCP connections provide the foundation for the DLSw communication.
2. After a connection is established, the DLSw partners exchange a list of supported capabilities in phase two. This helps to ensure that the peers use the same options. This is particularly vital when the DLSw partners are manufactured by different vendors.
3. Next, the DLSw partners establish circuits between SNA or NetBIOS end systems, and information frames can flow over the circuit.

A vulnerability exists in certain Cisco IOS software releases when configured for DLSw. After the connection is established, it is possible for a reload to occur should the device receive an invalid option during the capabilities exchange.

This vulnerability is documented in Cisco Bug ID [CSCsf28840](#) ([registered](#) customers only) .

Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability

Scoring System (CVSS).

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

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

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

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>.

CSCsf28840 (registered customers only)						
CVSS Base Score - 3.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal
CVSS Temporal Score - 2.7						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

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

☐ Impact

Successful exploitation of the vulnerability may result in a reload of the device.

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

☐ Software Version 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) describes a release train and the platforms or

products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. 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. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL:
<http://www.cisco.com/warp/public/620/1.html>.

Major Release	Availability of Repaired Releases	
	Rebuild	Maintenance
Affected 12.0-Based Release		
12.0	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.0S		12.0(18)S
12.0SZ	Vulnerable; migrate to 12.0(23)S or later	
12.0T	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.0WC	12.0(5)WC17	
12.0XA	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.0XC	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.0XD	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.0XE	Vulnerable; migrate to 12.1(26)E8	
12.0XG	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.0XH	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.0XI	Vulnerable; migrate to 12.2(46); available 10-May-07	

12.0XJ	12.0(4)XJ5	
12.0XK	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.0XN	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.0XQ	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.0XR	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.0XT	Vulnerable; contact TAC	
Affected 12.1-Based Release	Rebuild	Maintenance
12.1	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.1AA	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.1E	12.1(26)E8	
	12.1(27b)E2; available 25-Jun-07	
12.1EC	Vulnerable; migrate to 12.2(4)BC1 or later	
12.1EX	Vulnerable; migrate to 12.1(26)E8	
12.1EZ	Vulnerable; migrate to 12.1(26)E8	
12.1T	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.1XA	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.1XC	Vulnerable; migrate to 12.2(46); available 10-May-07	
	Vulnerable; migrate to	

12.1XD	12.2(46); available 10-May-07	
12.1XE	12.1(1)XE1	
12.1XG	Vulnerable; migrate to 12.3(21) or later	
12.1XH	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.1XI	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.1XJ	Vulnerable; migrate to 12.3(21) or later	
12.1XM	Vulnerable; migrate to 12.3(21) or later	
12.1XP	Vulnerable; migrate to 12.3(21) or later	
12.1XQ	Vulnerable; migrate to 12.3(21) or later	
12.1XS	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.1XT	12.1(3)XT2	
12.1XV	12.1(5)XV1	
12.1XW	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.1XX	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.1XY	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.1XZ	Vulnerable; migrate to 12.2(46); available 10-May-07	
12.1YA	Vulnerable; migrate to 12.3(21) or later	
12.1YB	Vulnerable; migrate to 12.3(21) or later	
12.1YD	Vulnerable; migrate to	

	12.3(21) or later	
12.1YI	Vulnerable; migrate to 12.3(21) or later	
Affected 12.2-Based Release	Rebuild	Maintenance
12.2		12.2(46); available 10-May-07
12.2B	Vulnerable; migrate to 12.4(12) or later	
12.2BW	Vulnerable; migrate to 12.3(21) or later	
12.2BY	Vulnerable; migrate to 12.4(12) or later	
12.2DD	Vulnerable; migrate to 12.4(12) or later	
12.2DX	Vulnerable; migrate to 12.4(12) or later	
12.2IXA	Vulnerable; migrate to 12.2(18)IXC or later	
12.2IXB	Vulnerable; migrate to 12.2(18)IXC or later	
12.2MC	Vulnerable; migrate to 12.4(12) or later	
12.2S		12.2(30)S
12.2SB	12.2(28) SB6	
	12.2(31) SB2	
12.2SBC	Vulnerable; migrate to 12.2(31)SB2 or later	
12.2SRA	12.2(33) SRA2	
12.2SU	Vulnerable; migrate to 12.4(12) or later	
12.2SV		12.2(26)SV
12.2SW	12.2(25) SW9	
12.2SX	Vulnerable; migrate to 12.2(18)SXE6b	
	Vulnerable; migrate to	

12.2SXA	12.2(18)SXE6b	
12.2SXB	Vulnerable; migrate to 12.2(18)SXE6b	
12.2SXD	Vulnerable; migrate to 12.2(18)SXE6b	
12.2SXE	12.2(18)SXE6b	
12.2SXF	12.2(18)SXF8	
12.2SY	Vulnerable; migrate to 12.2(18)SXE6b	
12.2SZ	Vulnerable; migrate to 12.2(30)S or later	
12.2T	Vulnerable; migrate to 12.3(21) or later	
12.2TPC	Vulnerable; contact TAC	
12.2XA	Vulnerable; migrate to 12.3(21) or later	
12.2XB	12.2(2)XB17	
12.2XC	Vulnerable; migrate to 12.4(12) or later	
12.2XD	Vulnerable; migrate to 12.3(21) or later	
12.2XG	Vulnerable; migrate to 12.3(21) or later	
12.2XH	Vulnerable; migrate to 12.3(21) or later	
12.2XJ	Vulnerable; migrate to 12.3(21) or later	
12.2XK	Vulnerable; migrate to 12.3(21) or later	
12.2XL	Vulnerable; migrate to 12.3(21) or later	
12.2XM	Vulnerable; migrate to 12.3(21) or later	
12.2XN	Vulnerable; migrate to 12.3(21) or later	
12.2XQ	Vulnerable; migrate to 12.3(21) or later	

12.2XT	Vulnerable; migrate to 12.3(21) or later	
12.2XU	Vulnerable; migrate to 12.3(21) or later	
12.2XV	Vulnerable; migrate to 12.3(21) or later	
12.2XW	Vulnerable; migrate to 12.3(21) or later	
12.2YA	12.2(4) YA10	
12.2YB	Vulnerable; migrate to 12.3(21) or later	
12.2YC	Vulnerable; migrate to 12.3(21) or later	
12.2YD	Vulnerable; migrate to 12.4(12) or later	
12.2YE	Vulnerable; migrate to 12.2(30)S or later	
12.2YF	Vulnerable; migrate to 12.3(21) or later	
12.2YH	Vulnerable; migrate to 12.3(21) or later	
12.2YJ	12.2(8)YJ1	
12.2YL	Vulnerable; migrate to 12.4(12) or later	
12.2YM	Vulnerable; migrate to 12.4(12) or later	
12.2YN	Vulnerable; migrate to 12.4(12) or later	
12.2YT	Vulnerable; migrate to 12.3(21) or later	
12.2YU	Vulnerable; migrate to 12.4(12) or later	
12.2YV	12.2(11) YV1	
12.2YW	Vulnerable; migrate to 12.4(12) or later	
12.2YX	Vulnerable; migrate to 12.4(12) or later	

12.2YY	Vulnerable; migrate to 12.4(12) or later	
12.2YZ	Vulnerable; migrate to 12.2(30)S or later	
12.2ZA	Vulnerable; migrate to 12.2(18)SXE6b	
12.2ZB	Vulnerable; migrate to 12.4(12) or later	
12.2ZD	Vulnerable; contact TAC	
12.2ZE	Vulnerable; migrate to 12.3(21) or later	
12.2ZF	Vulnerable; migrate to 12.4(12) or later	
12.2ZH	12.2(13) ZH6	
12.2ZJ	Vulnerable; migrate to 12.4(12) or later	
12.2ZL	Vulnerable; contact TAC	
12.2ZN	Vulnerable; migrate to 12.4(12) or later	
12.2ZP	Migrate to 12.2(20)S7 or later	
12.2ZU	Vulnerable; contact TAC	
12.2ZV	12.2(28a) ZV1	
12.2ZW	Vulnerable; migrate to 12.2(33)SRB	
12.2ZX		12.2(28)ZX
Affected 12.3-Based Release	Rebuild	Maintenance
12.3		12.3(21)
12.3B	Vulnerable; migrate to 12.4(12) or later	
12.3BW	Vulnerable; migrate to 12.4(12) or later	
12.3T	Vulnerable; migrate to 12.4(12) or later	
12.3XA	12.3(2)XA5	
12.3XB	Vulnerable; migrate to 12.4(12) or later	

12.3XC	12.3(2)XC3	
12.3XD	Vulnerable; migrate to 12.4(12) or later	
12.3XE	12.3(2)XE2	
12.3XF	Vulnerable; migrate to 12.4(12) or later	
12.3XG	Vulnerable; contact TAC	
12.3XH	Vulnerable; migrate to 12.4(12) or later	
12.3XI	12.3(7) XI8a	
12.3XJ	Vulnerable; migrate to 12.4(11)T1	
12.3XK	Vulnerable; migrate to 12.4(12) or later	
12.3XQ	Vulnerable; migrate to 12.4(12) or later	
12.3XR	Vulnerable; contact TAC	
12.3XU	Vulnerable; migrate to 12.4(4)T7 or later	
12.3XW	Vulnerable; migrate to 12.4(11)T1	
12.3XX	12.3(8)XX2	
12.3YF	Vulnerable; migrate to 12.4(11)T1	
12.3YG	12.3(8)YG5	
12.3YH	Vulnerable; migrate to 12.4(4)T7 or later	
12.3YI	Vulnerable; migrate to 12.4(4)T7 or later	
12.3YJ	Vulnerable; migrate to 12.4(6)T6 or later	
12.3YK	Vulnerable; migrate to 12.4(4)T7 or later	
12.3YM	Vulnerable; contact TAC	
12.3YQ	Vulnerable; migrate to 12.4(6)T6 or later	
12.3YT	Vulnerable; migrate to 12.4(4)T7 or later	

12.3YU	Vulnerable; contact TAC	
12.3YX	Vulnerable; migrate to 12.4(11)T1	
12.3YZ	Vulnerable; contact TAC	
Affected 12.4-Based Release	Rebuild	Maintenance
12.4	12.4(7d)	
	12.4(8c)	
	12.4(10a)	12.4(12)
12.4T	12.4(4)T7	
	12.4(6)T6	
	12.4(9)T3	
	12.4(11)T1	
12.4XA	Vulnerable; migrate to 12.4(6)T6 or later	
12.4XB	Vulnerable; contact TAC	
12.4XC	12.4(4)XC6	
12.4XD	12.4(4)XD5	
12.4XE	Vulnerable; contact TAC	

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

☐ Workarounds

The effectiveness of any mitigation 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 mitigation or fix is the most appropriate for use in the intended network before it is deployed.

Additional mitigations 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-20070110-dlsw.shtml>

Configure Explicitly Defined DLSw Peers

If DLSw is configured with no remote peers defined, then it must be operating in promiscuous mode on one end of the connection. Promiscuous mode could allow for any device to attempt to establish a DLSw peer with the router. To prevent malicious connections, DLSw peers may be explicitly defined with the **dlsw remote-peer** command removing the need for promiscuous mode.

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

☐ **Obtaining Fixed Software**

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. 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/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

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

☐ **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>.

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

☐ **Customers using Third Party Support Organizations**

Customers whose Cisco products are provided or maintained through prior or existing agreement 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.

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

☐ **Customers without Service Contracts**

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their 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

Have your product serial number available and give the URL of this notice as evidence of your 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 special localized telephone numbers and instructions and e-mail addresses for use in various languages.

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

☐ **Exploitation and Public Announcements**

This vulnerability was reported to Cisco by Martyn Ruks of MWR InfoSecurity and was originally presented at DEFCON in August 2006.

[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-20070110-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
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu

- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- 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 1.2	2007- April-20	Corrected release information and dates, especially for 12.2(46) fixes.
Revision 1.1	2007- January-12	Corrected release dates for 12.4 (11)T1
Revision 1.0	2007- January-10	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. 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](#)

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

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).