

MWR InfoSecurity Advisory

Cisco IOS
Invalid DLSw Handshake
Denial of Service

10th January 2007

MWR  INFOSECURITY

CONTENTS

Cisco IOS Invalid DLSw Handshake Denial of Service	3
1. Detailed Vulnerability Description	4
1.1. Introduction	4
1.2. Technical Background	5
1.3. Exploit Information	8
1.4. Dependencies	10
2. Recommendations	12
3. References	13



Cisco IOS Invalid DLSw Handshake Denial of Service

Package Name: Cisco Internetworking Operating System

Date: 2007-01-10

Affected Versions: Cisco IOS versions 11.0 through 12.4.

CVE Reference: Not yet submitted

Date: 2007-01-10

Severity: Medium Risk

Local/Remote: Remote

Vulnerability Class: Denial of Service

Vendor URL: www.cisco.com

Vendor Response: Issue reported to vendor August 6th 2006. MWR InfoSecurity and Cisco have worked together such that full details of the vulnerability were disclosed through appropriate channels.

Exploit Details Included: Yes

Affected OS: Cisco IOS (please refer to Cisco advisory for full product matrix)

Dependencies: A number of conditions must be met for this vulnerability to be exploited; these are described within this document.

Overview: Data Link Switching is primarily used for transporting SNA communications across an IP network. Support for this protocol is provided by Cisco networking devices as part of IOS although it is not enabled by default. In specific configurations an attacker could use the DLSw service to trigger a reload of the router's configuration resulting in a Denial of Service condition.

Impact: The vulnerability allows an attacker to create a Denial of Service condition in a router that is running the DLSw service. Such a condition may be caused by triggering a reload of the device. The only confirmed mechanism for triggering this reload is by issuing a specific non-privileged command on the routing device. It is possible that other vectors exist for causing a reload once an invalid DLSw handshake has occurred.

Cause: The vulnerability is the result of inadequate checking on the data included within a specific parameter in a DLSw capability exchange. When this data is subject to further processing it causes an unhandled exception which results in a reload.

Interim Workaround: The ability to perform a DLSw capability exchange should be limited to trusted IP addresses only. Promiscuous mode should be disabled on all routing devices to prevent exploitation of this and other security related issues. Access to TCP port 2065, 2067 and other DLSw related services should also be restricted, either by the use of network filtering controls or Access Control Lists.

Solution: The vendor has issued upgraded versions of IOS that resolve the issue, please see the links within this document for further information.

Detailed Vulnerability Description

1. Introduction

Data Link Switching (DLSw) is a technology developed during the 1990s that allows the encapsulation of SNA and NetBIOS traffic across an IP network. Cisco describe the support they provide for this service as follows: -

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. It serves as an alternative to source-route bridging (SRB), a protocol for transporting SNA and NetBIOS traffic in Token Ring environments that was widely deployed before the introduction of DLSw. In general, DLSw addresses some of the shortcomings of SRB for certain communication requirements—particularly in WAN implementations. Cisco supports a third version of DLSw called DLSw+. DLSw+ is fully compliant with RFC 1795. The enhancements may be used when both peers are Cisco devices running DLSw+.

Reference: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/dlsw.htm

The DLSw protocol (Cisco designate their current implementation of the protocol as DLSw+) is typically used in environments supporting IBM networking technologies with the most common usage being to extend SNA access to mainframes across corporate IP based networks.

DLSw is used to bridge the previously described protocols across an IP network and requires pairs of routing devices to establish TCP connections between each other. To establish these connections an exchange of capabilities occurs so that further communication can be supported between the devices.

A vulnerability was identified when an invalid parameter was included within one of the capabilities exchanged during this process. Due to incorrect checking of the data, unexpected conditions can be encountered when further processing of this data occurs. In certain circumstances this results in the routing device performing a reload and it is therefore unavailable for the time taken for the reload to complete.

2. Technical Background

Data Link Switching (DLSw) is a protocol that was initially designed by IBM and was released in 1993. The original specification of the protocol was documented in RFC 1434.

The protocol is used for “packet switching” across an IP network through the use of encapsulation within a TCP connection. It is capable of handling the transport of SNA and NetBIOS frames and also provides the benefit of local termination of the link layer. This prevents the link layer management traffic from traversing the IP network which usually includes a WAN. This improves reliability and reduces the amount of traffic passing across the connections.

A number of improvements were made to the DLSw protocol during the early 1990s and were included in the next documentation of the protocol (RFC 1795) which was released in 1995.

Cisco produced their own extensions to the protocol known as DLSw+ and a large number of the features of this version were included within version 2 of the protocol. This was documented in RFC 2166 and was released in 1997. No further public developments have been made to the protocol and in practical terms DLSw+ is the most widely adopted form.

A DLSw packet can be divided into two main parts, the header section and the data section. An example of a DLSw packet can be observed in the screenshot included here: -

```

▼ Data Link SWitching
  ▼ DLSw header, Version 1 (RFC 1795)
    Version      = Version 1 (RFC 1795)
    Header Length = 72
    Message Length = 4
    Remote DLC   = 65546
    Remote DLC PID = 1383036276
    Reserved
    Message Type = Capabilities Exchange (0x20)
    Not used for CapEx
    Protocol ID  = 0x42
    Header Number = 0x01
    Not used for CapEx
    Old message type = Unknown Type (0x01)
    Not used for CapEx
    Frame direction = Capabilities response (0x02)
    Not used for CapEx
  ▼ DLSw data - Response Capabilities GDS
    Capabilities Length = 4
    Response Capabilities GDS
  
```

```

0050 04 ac 10 0a 34 00 03 00 0d 45 74 68 02 72 6e 65  ....4... Ethrnet
0060 00 00 00 04 00 08 00 00 00 01 00 05 00 d6 43 69  ....0...Cl
0070 73 63 6f 20 49 6e 74 65 72 6e 65 74 77 6f 00 04  sco.inte.rnetwo..
0080 15 21
  
```

This example shows a type of packet known as a Capabilities Exchange Response and is only one possible type of DLSw message.

The purpose of each type of message is documented within the relevant RFCs but the most common types are listed here: -

- Capabilities Exchange
- CANUREACH
- ICANREACH
- XID
- Data
- Halt Data Link

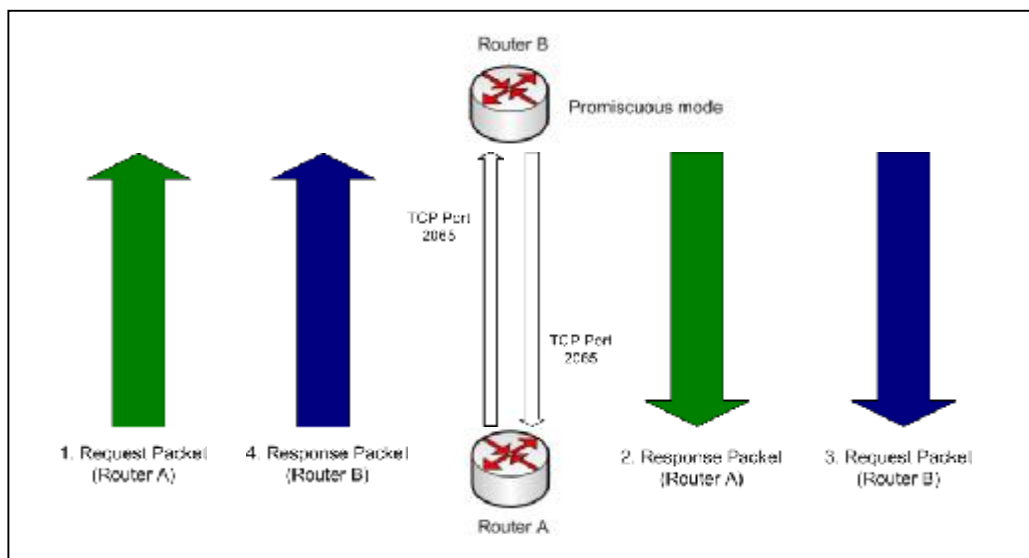
In order for SNA or NetBIOS data to pass across a DLSw connection a number of handshakes must occur. The initial handshake performed between two DLSw enabled devices is known as a Capabilities Exchange and is used to communicate the abilities of the DLSw devices to each other.

To perform such an exchange the configuration of the remote router needs to include one of the following assignments: -

- Promiscuous mode – this enables any device to perform the capabilities exchange and in the majority of environments one router will be configured in this manner.

- Static mode – this defines static IP addresses that can perform the exchange and can be configured to allow routers to connect to the device or the device to connect out to a remote system.

The diagram included here highlights the Capabilities Exchange process and the packets that must be sent by each device. In this example the attacker is the device labelled Router A and the target is labelled Router B.



In the diagram the packets coloured green relate to the capabilities request and response for Router A. The request and response relating to Router B are coloured blue.

As can be observed two TCP connections are set up between the devices, one in either direction. Each party must send their capabilities to the remote device using the connection they initiated. Each request must be answered with a successful response for the DLSw connection to be successfully established. This requires each device to support the capabilities advertised in the relevant request.

If version 2 of the protocol is used the initial connection made by the attacker will be closed by the remote device once the connection is established and all further communication occurs over a single TCP connection.

Once the Capabilities have been exchanged individual NetBIOS or SNA communications can then be established across the TCP connection and are known as DLSw circuits. These require another handshake to be performed to establish each circuit. However, a discussion of this aspect of the protocol is beyond the scope of this document.



Each capability is included within the data section of the handshake packet and takes the form of a Control Vector consisting of type LT structured subfields. The format of each capability is included here: -

```
Capability Type: 1 byte field (documented values can be found within RFC 1795)
Field Length: 1 byte (the length of the vector control block)
Data Value: Variable length (the length is determined by the previous byte)
```

Further information about the format of capability data can be discovered within the RFCs relating to DLSw as described previously.

Aside from the vulnerability described in this document, the ability to perform a DLSw Capabilities Exchange with another device exposes a number of risks to the environment. These include: -

- the ability to fingerprint the version of software running on the remote device
- information about supported SAP types
- MAC address and NetBIOS name information
- various other technical details

In addition, the ability to participate in the DLSw environment can also enable an attacker to perform traffic redirection attacks and create other types of disruption to the environment. These attacks are documented in the MWR InfoSecurity DEFCON 14 presentation^[2].

2.1. Exploit Information

The vulnerability can be exploited by an attacker who is capable of performing a Capabilities Exchange with a vulnerable router and then triggering a reload.

A Cisco routing device configured in DLSw promiscuous mode can typically be identified by lines similar to the following appearing in the configuration file.

```
source-bridge ring-group 1
dlsw local-peer peer-id 192.168.10.4 group 1 border promiscuous
dlsw remote-peer 0 tcp 192.168.10.1
```

Additionally, a DLSw enabled router can typically be identified by the TCP services that are running. The following data includes the results of a port scan conducted against a router with DLSw support enabled.

```
(The 65529 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
23/tcp    open  telnet
79/tcp    open  finger
80/tcp    open  http
1981/tcp  open  unknown
1982/tcp  open  unknown
```



```
1983/tcp open  unknown
2065/tcp open  dlsrpn
```

In the output above, the services typically associated with the DLSw protocol are highlighted in bold type.

Once a DLSw enabled router has been identified it is necessary to complete a Capabilities Exchange. The error conditions occur when a specific parameter is set in the capabilities exchange that is not expected by the remote device. The parameter that must be set in the data portion of the Capabilities Exchange Request packet is described here: -

```
Capability Name: Peer Type
Capability Value: d8h
Field Length: 3h
Data Value: f8h (most values other than 0, 1, 2 and 3 also work)
```

It should be noted that the Capabilities Exchange must be successfully completed and therefore a correctly formed packet must be used. A Cisco router will reject the Capability Exchange in the following circumstances: -

- The correct interface defined for DLSw communication is not used (usually the router's loopback interface).
- The values in the capabilities fields are not of expected lengths and values (except for the affected parameter).
- The length fields within the DLSw header and data portions of the packet are not calculated correctly.

To cause the Denial of Service it is necessary for the DLSw connection to remain open until the condition is triggered. This means that an attacker must keep both TCP connections open which requires that DLSw status responses be returned to the remote system when status requests are sent to the attacker. The format of a valid Cisco status response packet is included here: -

```
81 1e 00 0c 00 00 00 00 00 00 00
```

One method for triggering the Denial of Service is to query the status of the DLSw connection from a valid login session on the device. This requires an attacker to possess the ability to issue the command "show dlsw cap". By default, this can be executed by an unprivileged user.

It is also possible that other vectors could be used to exploit this issue; however, none have been documented at this time.

The result of executing this command on a vulnerable system can be observed here:

```
Router>show dls w cap
DLsw: Capabilities for peer 172.16.10.57(2065)
 vendor id (OUI)       : '00C' (cisco)
 version number       : 1
 release number       : 0
 init pacing window   : 20
 unsupported saps     : none
 num of tcp sessions  : 1
 loop prevent support : no
 icanreach mac-exclusive : no
 icanreach netbios-excl. : no
 reachable mac addresses : none
 reachable netbios names : none
 V2 multicast capable : yes
 DLsw multicast address : none
 cisco version number : 1
 peer group number    : 5
 border peer capable  : yes
 peer cost            : 2
 biu-segment configured : no
 UDP Unicast support  : no
 NetBIOS Namecache length : 15
 local-ack configured : yes
 priority configured  : no
--More--
Buffered messages:

00:01:00: %SYS-5-CONFIG_I: Configured from memory by console
00:01:00: %LINK-3-UPDOWN: Interface Ethernet0, changed state to up
00:01:00: %LINK-5-CHANGED: Interface Serial0, changed state to administratively down
00:01:00: %LINK-5-CHANGED: Interface Serial1, changed state to administratively down
00:01:00: %SYS-5-RESTART: System restarted --
```

To exploit this issue the following steps must therefore be completed by an attacker: -

- Perform a capabilities exchange with the target router with the “Peer Type” parameter set to an unexpected value such as “f8h”.
- Trigger the reload by issuing a “show dls w cap” command (or force another error condition).

2.2. Dependencies

There are a number of dependencies in the ability for an attacker to exploit this issue and these are outlined within this section. These are documented here so that it is possible to accurately assess the risk posed by this vulnerability in specific environments.

- DLsw must be enabled on the device and must be configured on an interface that is accessible by the attacker.



- TCP port 2065 and 2067 on the appropriate interface's IP address must be accessible by the attacker. Additionally, TCP port 2065 or 2067 on the attacker's system must also be reachable by the target device as a two way communication must be established.
- Promiscuous mode must be enabled on the device or an attacker must be able to use an IP address defined within the target's configuration file.
- An attacker must have the ability to trigger the condition. A user or administrator running the "show dlsw cap" command will definitely cause the router reload. Other vectors might also exist for triggering this condition either locally or remotely.



3. Recommendations

It is recommended that the appropriate vendor produced updates be installed to all vulnerable devices. Please refer to the Cisco advisory document at the following location: -

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

In addition to applying all security updates it is recommended that other best practice DLSw security measures be implemented within the environment. These include not using promiscuous mode and using network filtering to control access to DLSw services on the device.

Cisco's advice on additional protective measures is located here: -

http://www.cisco.com/en/US/products/products_security_response09186a00807bd13d.html

4. References

[1] Cisco Advisory: -

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

[2] MWR InfoSecurity IBM Networking Presentation – DEFCON 14

<http://www.mwrinfosecurity.com/news/1637.html>

[3] Cisco additional protective measures and mitigation techniques: -

http://www.cisco.com/en/US/products/products_security_response09186a00807bd13d.html

[4] Cisco outline of DLSw support: -

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/dlsw.htm

MWR InfoSecurity
St. Clement House
1-3 Alencon Link
Basingstoke, RG21 7SB
Tel: +44 (0)1256 300920
Fax: +44 (0)1256 844083
mwrinfosecurity.com