

Cisco Security Notice: Response to BugTraq – CDP Issue

Document ID: 60595

Revision 1.0

Last Updated 2001 October 12

Please provide your feedback on this document.

[Summary](#)
[Details](#)
[Cisco Security Procedures](#)

Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time.

Details

Original Report: <http://www.securityfocus.com/archive/1/273421> and <http://www.phenoelit.de/stuff/CiscoCDP.txt>. Cisco responded with the following, which is also archived at http://www.cisco.com/warp/public/707/cdp_issue.shtml:

There is a vulnerability in how Cisco routers and switches are handling Cisco Discovery Protocol (CDP). By sending a large amount of CDP neighbor announcements, it is possible to consume all of an available device's memory, causing a crash or some other abnormal behavior. This vulnerability is assigned the Cisco bug ID CSCdu09909 for Cisco IOS, and CSCdv57576 for CatOS. This vulnerability was discovered by fx@phenoelit.de.

All releases, prior fixed releases, of IOS and CatOS are vulnerable. All Catalyst models are vulnerable.

To follow the bug ID links below and see detailed bug information, you must be a registered user and you must be logged in.

- [CSCdu09909](#)
- [CSCdv57576](#)

In order to trigger this vulnerability, an attacker must be on the same segment as the target device. This vulnerability can not be exploited over the Internet unless an attacker has a helper program already planted on the internal network.

The workaround for this vulnerability is to disable CDP. CDP can be disabled either for the whole device or

on a selected links. In order to disable CDP for the whole router, execute the following global command:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no cdp run
```

Alternatively, CDP can be disabled on a particular interface. This can be done using the following commands:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface Ethernet0
Router(config-if)# no cdp enable
```

To disable CDP for the whole Catalyst, execute the following command:

```
Console> (enable) set cdp disable
```

Alternatively, CDP can be disabled on a particular interface. In this example CDP is disabled for the port 23 on a module 1:

```
Console> (enable) set cdp disable 1/23
```

In this particular case, Cisco Systems advises all customers to disable CDP for the whole device. If you must keep CDP running for any purpose then you should consider disabling it on all interfaces/ports that are facing host farms or outward of your administrative domain (for example, toward an upstream Internet Service Provider (ISP) or xdigital subscriber line (xDSL) customers).

This vulnerability has been fixed in the following interim Cisco IOS® Software releases:

- 12.2(3.6)B
- 12.2(4.1)S
- 12.2(3.6)PB
- 12.2(3.6)T
- 12.1(10.1)
- 12.2(3.6)

All later Cisco IOS releases should contain this fix.

Please note that interim images are built at regular intervals between maintenance releases and receive less testing. Interim images should be selected only if there is no other suitable release that addresses the vulnerability, and interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available through manufacturing, and usually they are not available for customer download from CCO without an earlier arrangement with the Cisco Systems Technical Assistance Center (TAC).

At this moment Cisco Systems does not have estimated dates when fixed versions of CatOS will be available.

Cisco Systems would like to thank Phenoelit on his cooperation on this issue.

Revision History		
Revision 1.0	2001–October–10	Initial public release.
Revision 1.1	2001–October–12	Added information about Catalyst.

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>.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Oct 12, 2001

Document ID: 60595
