

Cisco Security Advisory: CBOS - Improving Resilience to Denial-of-Service Attacks

Advisory ID: cisco-sa-20020523-cbos-dos

<http://www.cisco.com/warp/public/707/cisco-sa-20020523-cbos-dos.shtml>

Revision 1.2

Last Updated 2002 June 17 2000 UTC (GMT)

For Public Release 2002 May 23 1600 UTC (GMT)

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

Contents

- [Summary](#)
- [Affected Products](#)
- [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

Three new vulnerabilities are identified in Cisco Broadband Operating System (CBOS), an operating system for the Cisco 600 family of routers. Each vulnerability can cause a Denial of Service (DoS) by freezing the customer premises equipment (CPE). All three vulnerabilities can be exploited remotely.

No other Cisco product is vulnerable.

Workarounds are provided for two of the three vulnerabilities. Note that the workarounds provided may not be applicable in all cases. See the [Workarounds](#) section for further details.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20020523-cbos-dos.shtml>.

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

☐ **Affected Products**

This section provides details on affected products.

☐ **Vulnerable Products**

All Cisco DSL CPE devices from the 600 family running CBOS software up to and including 2.4.4 release are vulnerable. The complete list of vulnerable hardware models is: 626, 627, 633, 673, 675, 675e, 676, 677, 677i and 678.

☐ **Products Confirmed Not Vulnerable**

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

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

☐ **Details**

This section details the vulnerabilities described in this document.

- **CSCdw90020** -- By sending a large packet to the Dynamic Host Configuration Protocol (DHCP) port it is possible to freeze the CPE. DHCP service is enabled by default.
- **CSCdv50135** -- By sending a large packet to the Telnet port it is possible to freeze the CPE. It is not necessary to be logged in or to authenticate in any way. Telnet is enabled by default.
- **CSCdx36121** -- The TCP/IP stack will consume all memory while processing received packets. This will happen only if the CPE must process a high number of overly large packets. These packets must have the CPE as the destination. After the memory is exhausted the CPE will lock up and stop forwarding any further packets.

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

☐ **Impact**

By repeatedly exploiting these vulnerabilities an attacker can cause a DOS for an indeterminate period of time.

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

☐ **Software Versions and Fixes**

All vulnerabilities are fixed in CBOS version 2.4.5 or later.

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

☐ Workarounds

This section describes workarounds for the vulnerabilities described in this document.

- **CSCdw90020** - The workaround is to filter DHCP requests. This task must be executed while in **enable** mode.

To filter DHCP packets use this procedure:

```
cbos# set filter 0 on allow incoming eth0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0
udp srcport 68-68 destport 67-67
cbos# set filter 1 on allow outgoing eth0 1.2.3.4 255.255.255.255 0.0.0
protocol udp srcport 67-67 destport 68-68
```

The filter "0" will allow all DHCP requests from your internal network to the CPE. The filter "1" will allow all DHCP responses from the CPE. In this example, the eth0 interface of the CPE has the IP address of 1.2.3.4. You must substitute this address with the IP address of your eth0 port. This configuration is not the complete workaround since you are still exposed from you LAN side (behind the eth0 interface).

Note: There is an implicit "deny all" as the last filter so you must include additional "permit" filters to allow a normal traffic flow. If you already have filters configured, you should combine this example with the configured filters and probably change the filter numbers to suit your configuration. Also note that this workaround is not applicable if you must have DHCP enabled on the WAN side.

For information regarding filters, refer to:

http://www.cisco.com/en/US/products/hw/modems/ps296/products_installation_guide_book09

- **CSCdv50135** - The workaround is to disable Telnet. This task must be executed while in **enable** mode. To disable Telnet use this procedure:

```
cbos# set telnet disable
cbos# write
```

- **CSCdx36121** - There is no workaround.

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

☐ Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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**

These vulnerabilities were reported by Knud Erik Højgaard from Cybercity, Denmark. The exploit code for CSCdv50135 was made public by a third party unrelated to Knud Højgaard in any way. This vulnerability was also publicly discussed.

[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 notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20020523-cbos-dos.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
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- firewalls@lists.gnac.com
- Various internal Cisco mailing lists

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

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

☐ **Revision History**

Revision 1.2	2002- June-17	Updated Software Versions and Fixes section
Revision 1.1	2002- May-31	Updated Affected Products section
Revision 1.0	2002- May-23	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](#)

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)

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

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

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