

Cisco Security Advisory: Multiple Vulnerabilities in CBOS

Document ID: 10925

Advisory ID: cisco-sa-20001204-cbos

<http://www.cisco.com/warp/public/707/cisco-sa-20001204-cbos.shtml>

Revision 1.5

Last Updated 2001 August 08 2100 UTC (GMT)

For Public Release 2000 December 04 0800 UTC (GMT)

Please provide your feedback on this document.

[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

Multiple vulnerabilities have been identified and fixed in CBOS, an operating system for the Cisco 600 family of routers.

- Any router in the Cisco 600 family that is configured to allow Web access can be locked by sending a specific URL. Web access is disabled by default, and it is usually enabled in order to facilitate remote configuration. This defect is documented as Cisco bug ID **CSCdr98772**.
- By sending a stream of TCP SYN packets to the router, it is possible to exhaust all available TCP sockets. The consequence is that no new TCP sessions addressed to the router will be established. The difference between this vulnerability and a SYN Denial-of-Service attack is that this one can be accomplished by a slow stream of packets (one per second). This defect is documented as Cisco bug ID **CSCds59206**.
- Invalid login attempts using the Web interface are not logged. This defect is documented as Cisco bug ID **CSCds19142**.

- It is possible to lock up the router by sending a large ICMP ECHO (PING) packet to it. This defect is documented as Cisco bug ID **CSCds23921**.

The following releases of CBOS are vulnerable to all defects: 2.0.1, 2.1.0, 2.1.0a, 2.2.0, 2.2.1, 2.2.1a, 2.3, 2.3.2, 2.3.5, 2.3.7 and 2.3.8.

These defects will be fixed in the following CBOS releases: 2.3.5.015, 2.3.7.002, 2.3.9 and 2.4.1. Customers are urged to upgrade to releases that are not vulnerable to this defect as shown in detail in the section Software Versions and Fixes below.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20001204-cbos.shtml>.

Affected Products

This section supplies details on affected products.

Vulnerable Products

The affected models are: 627, 633, 673, 675, 675E, 677, 677i and 678.

These models are vulnerable if they run any of the following, or earlier, CBOS releases: 2.0.1, 2.1.0, 2.1.0a, 2.2.0, 2.2.1, 2.2.1a, 2.3, 2.3.2, 2.3.5, 2.3.7 and 2.3.8.

These defects will be fixed in the following CBOS releases: 2.3.5.015, 2.3.7.002, 2.3.9 and 2.4.1.

Products Confirmed Not Vulnerable

No other releases of CBOS software are affected by this vulnerability. No other Cisco products are affected by this vulnerability.

Details

CSCdr98772

The behavior is caused by inadequate URL parsing in CBOS. Each URL was expected to terminate with a minimum of a single space character (ASCII code 32, decimal). Sending a URL that does not terminate with a space causes CBOS to enter an infinite loop. It is necessary to power cycle the router to resume operation. To exploit this vulnerability, a router must be configured to accept Web connections. Having a Web access password configured does not provide protection against this vulnerability.

CSCds59206

By sending a stream of SYN packets addressed to the router, it is possible to exhaust all available TCP sockets within CBOS. This is due to the memory leak in CBOS. When a router is set into a state where it cannot accept a new connection, it can be maintained in this state by a slow stream of SYN packets until the router is rebooted. The stream can be as slow as one packet per second, so one machine with a 64 KB connection can hold up approximately 150 routers.

Note: This does not effect non-TCP traffic. All User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) packets can be handled by a router without any problems. All existing and new TCP sessions through the router will not be affected.

When an attacking stream is terminated, a router recovers itself within a few minutes.

CSCds19142

Using the Cisco Web Management interface, it is possible to keep guessing an access password without those password attempts being logged. A password may be either "exec-only" or "enable". A user with an "exec-only" password cannot change a router configuration.

CSCds23921 By sending a large (at least 65500 bytes in size) ICMP ECHO (PING) packet to the router itself, it is possible to overflow an internal variable and cause router lockup. The router is not affected by the packets which are routed through it.

Impact

CSCdr98772

By sending a tailored URL to a router, it is possible to cause a Denial-of-Service. Every affected router must be powered off and back on in order to restore its normal functionality.

CSCds59206

It is possible to prevent all TCP access to a router. This blocks all attempts at remote router administration.

CSCds19142

Long term, brute force password guessing can be performed without being noticed. When the correct password is guessed, it can be used to view or modify router configuration. This may be particularly dangerous in installations where multiple routers have the same password.

CSCds23921

It is possible to lock up the router thus causing Denial-of-Service. Every affected device must be powered off and back on in order to restore its normal functionality.

Software Versions and Fixes

The following table summarizes the CBOS software releases affected by the defects described in this notice and scheduled dates on which the earliest corresponding fixed releases will be available. Dates are tentative and subject to change.

Major Release	Description or Platform	Availability of Repaired Releases*	
		Patch release**	General Availability (GA)
All releases	627, 633, 673, 675, 677, 678	2.3.5.015 2000-DEC-15	-
2.3.7.001	677i	2.3.7.002	-

		2000-DEC-15	
All releases	All platforms	-	2.3.9 2001-MARCH 19
All releases	All platforms	-	2.4.1 2000-DEC-15
Notes			
* All dates are estimated and subject to change.			
** Patch releases are subjected to less rigorous testing than regular GA releases, and may have serious bugs.			

Workarounds

CSCdr98772

There are two workarounds for this vulnerability. The potential for exploitation can be lessened by ensuring that Web access to the router is limited to a legitimate IP address.

This can be done by entering the following commands while in **enable** mode:

```
cbos# set web remote 10.0.0.1
cbos# set web enabled
```

where 10.0.0.1 is the address of the host with a legitimate need for Web access to the router.

Alternatively, disabling the Web access completely will also prevent this vulnerability from being exploited. This can be done by entering the following command while in enable mode:

```
cbos# set web disabled
```

Another option is to change the Web port from the default port 80 to some arbitrary port. This will also help in cases where malicious program is making HTTP requests to the default port. This can be accomplished by the following commands:

```
cbos# set web port <arbitrary_port_greater_than_1024>
cbos# write
cbos# reboot
```

You *must* reboot the router in order for changes to take effect. You should also take care to avoid well known ports that are described in RFC1700.

CSCds59206

There is no workaround for this vulnerability.

CSCds19142

The Web Management interface can be disabled by entering the following commands in **enable** mode:

Cisco Security Advisory: Multiple Vulnerabilities in CBOS

```
cbos# set web disabled
```

CSCds23921

All incoming ICMP ECHO (PING) packets destined to the router itself should be denied. That can be achieved by following commands:

```
cbos# set filter number on deny incoming all 0.0.0.0 0.0.0.0 <eth0_IP_address> 255.255.255.255
cbos# set filter number+1 on deny incoming all 0.0.0.0 0.0.0.0 <wan0_IP_address> 255.255.255.255
```

Where *number* is a free filter number between 0 and 17.

Obtaining Fixed Software

Cisco is offering free software upgrades to eliminate this vulnerability for all affected customers.

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 Web site at <http://www.cisco.com>.

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 assistance with the upgrade, which should be free of charge.

Customers without Service Contracts

Customers without contracts 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

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

Exploitation and Public Announcements

The vulnerability CSCdr98772 was discovered by several customers. It was also discussed at public forums. PSIRT has received reports that this vulnerability has been exploited in vivo.

The vulnerability CSCds23921 was discovered by a customer. The other two vulnerabilities (CSCds59206 and CSCds19142) were discovered during internal testing.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements of

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.

Distribution

This advisory is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20001204-cbos.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.

Revision History

1.5	2001-August-08	Updated Workarounds Section.
1.4	2001-March-19	Updated GA for release 2.3.9; changed status from interim to final.
1.3	2000-December-19	Removed instructions for temporarily accessing fixed software images; removed text under CSCdr98772 about Web access on Cisco 600 routers.
1.2	2000-December-13	Updated software availability date, and added instructions for obtaining software.
1.1	2000-December-10	Updated software availability date, and added instructions on requesting assistance from third-party support

		organizations in the Obtaining Fixed Software section.
1.0	2000–December–03	Draft for initial public release.

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: Aug 08, 2001

Document ID: 10925
