CERT Advisory CA-1992-20 Cisco Access List Vulnerability

Original issue date: December 10,1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file. The CERT Coordination Center has received information concerning a vulnerability with Cisco routers when access lists are utilized. This vulnerability is present in Cisco software releases 8.2, 8.3, 9.0 and 9.1.

Systems and CERT strongly recommend that sites using Cisco routers for firewalls take immediate action to eliminate this vulnerability from their networks.

This vulnerability is fixed in Cisco software releases 8.3 (update 5.10), 9.0 (update 2.5), 9.1 (update 1.1) and in all later releases. Customers who are using software release 8.2 and do not want to upgrade to a later release should contact Cisco's Technical Assistance Center (TAC) at 800-553-2447 (Internet: tac@cisco.com) for more information.

The following interim releases are available via anonymous FTP from ftp.cisco.com (131.108.1.111).

Note: this FTP server will not allow filenames to be listed or matched with wildcards. You also cannot request the file by its full pathname. You must first cd to the desired directory (beta83_dir, beta90_dir, or beta91_dir) and then request the file desired (gs3-bfx.83-5.10, etc.).

Release (Update)	Filename	Size	Checksum
8.3 (5.10)	/beta83_dir/gs3-bfx.83-5.10	1234696	02465 1206
9.0 (2.5)	/beta90_dir/gs3-bfx.90-2.5	1705364	47092 1666
9.1 (1.1)	/beta91_dir/gs3-k.91-1.1	2005548	59407 1959

These releases are also available on Cisco's Customer Information On-Line (CIO) service for those customers having a maintenance contract. Other customers may obtain these releases through Cisco's Technical Assistance Center or by contacting their local Cisco distributor.

I. Description

A vulnerability in Cisco access lists allows some packets to be erroneously routed which one would expect to be filtered by the access list and vice-versa. This vulnerability can allow unauthorized traffic to pass through the gateway and can block authorized traffic.

II. Problem

If a Cisco router is configured to use extended IP access lists for traffic filtering on an MCI, SCI, cBus or cBusII interface, and the IP route cache is enabled, and the "established" keyword is used in the access list, then the access list can be improperly evaluated. This can permit packets which should be filtered and filter packets which should be permitted.

III. Workaround

This vulnerability can be avoided by either rewriting the extended access list to not use the "established" keyword, or by configuring the interface to not use the IP route cache. To disable the IP route cache, use the configuration command "no ip route-cache".

Example for a serial interface:

```
        router>enable


        Password:
        router#configure terminal

        Enter configuration commands, one per line.
        Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
        interface serial 0
        no ip route-cache
        ^Z
        router#write memory
```

IV. Solution

Obtain and install the appropriate interim release listed above. Sites which are not experienced at this installation process should contact the TAC center at 800-553-2447 for assistance.

The CERT Coordination Center wishes to thank Keith Reynolds of the Santa Cruz Operation for his assistance in identifying this problem and Cisco Systems for their assistance in providing technical information for this advisory.

Revision History

```
September 19,1997  Attached copyright statement
```