CERT Advisory CA-2003-17 Exploit available for for the Cisco IOS Interface Blocked Vulnerabilities

Original release date: July 18, 2003
Last revised: --
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- All Cisco devices running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets

Overview

An exploit has been posted publicly for the vulnerability described in VU#411332, which was announced in

http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

I. Description

An exploit has been posted publicly for VU#411332. This exploit allows an attacker to interrupt the normal operation of a vulnerable device. We believe it is likely that intruders will begin using this or other exploits to cause service outages.

Many large service providers have already taken action or are in the midst of upgrading. However, if you have not already taken action, we strongly encourage you to review the advisory provided by Cisco and take action in accordance with your site's maintenance and change management procedures. Cisco's advisory can be found at

> *http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml*

The CERT/CC will continue to provide information about this vulnerability through VU#411332.

Any information regarding intruder activity related to this vulnerability will be posted to the CERT/CC Currect Activity page, available at

> *http://www.cert.org/current/*

II. Impact

By sending specially crafted IPv4 packets to an interface on a vulnerable device, an intruder can cause the device to stop processing packets destined to that interface. Quoting from Cisco's advisory:

> *A device receiving these specifically crafted IPv4 packets will force the inbound interface to stop processing traffic. The device may stop processing packets destined to the router, including routing protocol packets and ARP packets. No alarms will be triggered, nor will the router reload to correct itself. This issue can affect all Cisco devices running Cisco IOS software. This vulnerability may be exercised repeatedly resulting in loss of availability until a workaround has been applied or the device has been upgraded to a fixed version of code.*

III. Solution

Apply a patch from Cisco

Upgrade as described in Cisco's Advisory.

Restrict access

Until a patch can be applied, you can mitigate the risks presented by this vulnerability by judicious use of access control lists (ACLs). The correct use of ACLs depends on your network topology. Additionally, ACLs may degrade performance on some systems. We recommend reviewing the following before applying ACLs:

> *http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml#workarounds*
> *http://www.cisco.com/warp/public/707/racl.html*
> *http://www.cisco.com/warp/public/707/iacl.html*

The CERT Coordination Center thanks Cisco Systems for notifying us about this problem and for helping us to construct this advisory.

Authors: Shawn Hernan and Martin Lindner

Revision History

```
July 18, 2003:  Initial release
```