



ADVISORY

Updated Information IOS Interface Blocked by IPv4 Packet
July 18, 2003

SYSTEMS AFFECTED: Routers and switches running Cisco IOS software.

OVERVIEW

The Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSD) is issuing this advisory to heighten awareness of a remotely exploitable vulnerability in Cisco IOS 10.3 or later.

DHS is working closely with the information technology industry to improve vulnerability awareness and information dissemination. DHS received confirmation that this vulnerability was exploited in a laboratory environment. Industry representatives have also verified that an exploit for this vulnerability exists in the wild. The probability of continued exploitation is high.

IMPACT

The recently announced vulnerability in devices running Cisco IOS 10.3 or later may be exploited to cause a denial of service state. Because routers and switches are an essential part of all network infrastructures, and because Cisco devices comprise a significant portion of those infrastructures, widespread exploitation of vulnerable Cisco devices could disrupt portions of the Internet. Rebooting the devices will restore availability. However, the devices are vulnerable to repeat exploits until corrections have been applied.

DETAILS

This vulnerability can be exploited by sending a string of specifically crafted IPv4 packets. 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.

RECOMMENDATION

Due to the seriousness of the Cisco IOS vulnerability and the availability of exploit code, DHS encourages administrators to take this opportunity to review the security of their Cisco systems implementation as soon as possible. DHS strongly recommends that system administrators who have not taken corrective action on Cisco devices do so now.

Cisco IOS upgrades, workarounds, and additional information are available from Cisco at: (<http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml>).

Advisories recommend the immediate implementation of protective actions, including best practices when available. DHS encourages recipients of this advisory to report information concerning suspicious or criminal activity to law enforcement or a DHS watch office. The DHS Information Analysis and Infrastructure Protection watch offices may be contacted at:

For private citizens and companies – Phone: (202) 323-3205, 1-888-585-9078,
Email: nipc.watch@fbi.gov;
Online: <http://www.nipc.gov/incident/cirr.htm>

For telecommunications industry - Phone: (703) 607-4950
Email: ncs@dhs.gov

For Federal agencies/departments - Phone: (888) 282-0870
Email: fedcirc@fedcirc.gov
Online: <https://incidentreport.fedcirc.gov>

DHS intends to update this alert should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory System (HSAS) is anticipated; the current HSAS level is YELLOW.