Cisco Security Advisory

Multiple Crafted IPv6 Packets Cause Reload

Advisory ID: cisco-sa-20050126-ipv6

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050126-ipv6

Revision 1.0

For Public Release 2005 January 26 16:00 UTC (GMT)

Contents

Summary

Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

Cisco has made free software available to address this vulnerability.

There are workarounds available to mitigate the effects.

This issue is tracked by CERT/CC VU#472582

This advisory is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050126-ipv6.

[Expand all sections] [Collapse all sections]

Affected Products

This section provides details on affected products.

Vulnerable Products

Only the Cisco devices running IOS and configured for IPv6 are affected. A router will display all IPv6

enabled interfaces with the **show ipv6 interface** command.

An empty output or an error message will be displayed if IPv6 is disabled or unsupported on the system. In this case the system is **not** vulnerable.

Sample output of **show ipv6 interface** command is shown below for a system configured for IPv6.

```
Router#show ipv6 interface Serial1/0 is up, line protocol is up IPv6 is
enabled, link-local address is FE80::A8BB:CCFF:FE00:D200 Global unicast
address(es): 2001:1:33::3, subnet is 2001:1:33::/64 [TENTATIVE] Joined group
address(es): FF02::1 FF02::1:FF00:3 FF02::1:FF00:D200 MTU is 1500 bytes ICMP
error messages limited to one every 100 milliseconds ICMP redirects are
enabled ND DAD is enabled, number of DAD attempts: 1 ND reachable time is
30000 milliseconds Router#
```

A router that has IPv6 enabled on a physical or logical interface is vulnerable to this issue even if **ipv6 unicast-routing** is globally disabled. The **show ipv6 interface** command can be used to determine whether IPv6 is enabled on any interface.

Products Confirmed Not Vulnerable

Products that are not running Cisco IOS are not affected.

Products running any version of Cisco IOS that do not have IPv6 configured interfaces are not vulnerable.

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

Top of the section Close Section

Details

IPv6 is the "Internet Protocol Version 6", designed by the Internet Engineering Task Force (IETF) to replace the current version Internet Protocol, IP Version 4 (IPv4).

A vulnerability exists in the processing of IPv6 packets that can be exploited to cause the reload of a system. Crafted packets received on logical interfaces (that is, tunnels including 6to4 tunnels) as well as physical interfaces can trigger this vulnerability.

Multiple crafted IPv6 packets need to be sent to exploit this vulnerability. Such crafted packets can be sent remotely.

This issue is documented in Cisco bug ID CSCed40933 (registered customers only) .

Top of the section Close Section

Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine

urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html .

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at http://intellishield.cisco.com/security/alertmanager/cvss .

Top of the section Close Section

Impact

Successful exploitation of this vulnerability results in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

Top of the section Close Section

Software Versions and Fixes

Major Release	Availability of Repaired Releases		
Affected 12.0-Based Release	**Rebuild**	**Interim**	**Maintenance**
12.0S	12.0(23)S and before are not vulnerable.		
	12.0(24)S6		
	12.0(25)S3		
	12.0(26)S2		

	12.0(27)S1		
			12.0(28)S
12.0SX	12.0(25)SX8		
12.0SZ	12.0(27)SZ		
Affected 12.2-Based Release	**Rebuild**	**Interim**	**Maintenance**
12.2B	12.2(2)B - 12.2(4)B7 Migrate to 12.2(13)T14 or later		
	12.2(4)B8 AND FWD Migrate to 12.3(7)T or later		
12.2BC	Migrate to 12.3(9a)BC		
12.2BX	Migrate to 12.3(7)XI1		
12.2BZ	Migrate to 12.3(7)XI1		
12.2CX	No plan.		
12.2CZ	No plan.		
12.2EW	12.2(18)EW1		
12.2EWA			12.2(20)EWA
12.2JK	12.2(15)JK2		

12.2MC	Migrate to 12.3(11)T		
12.2S	12.2(14)S9		
	12.2(18)S5		
	12.2(20)S3		
	12.2(22)S1		
			12.2(25)S
12.2SE	12.2(25)SE		
12.2SU	12.2(14)SU1		
12.2SV	12.2(23)SV		
12.2SW	12.2(23)SW		
12.2SX	Migrate to 12.2(17d)SXB2 or later		
12.2SXA	Migrate to 12.2(17d)SXB1 or later		
12.2SXB	12.2(17d)SXB1		
12.2SXD			12.2(18)SXD
12.2SY	Migrate to 12.2(17d)SXB2 or later		
12.2SZ	Migrate to 12.2(20)S4		

12.2T	12.2(13)T14		
	12.2(15)T12		
12.2YT	Migrate to 12.2(15)T13 or later		
12.2YU	Migrate to 12.3(4)T6 or later		
12.2YV	Migrate to 12.3(4)T6 or later		
12.2YZ	Migrate to 12.2(20)S4 or later		
12.2ZC	Migrate to 12.3T or later		
12.2ZD	Migrate to 12.3 or later		
12.2ZE	Migrate to 12.3 or later		
12.2ZF	Migrate to 12.3(4)T6 or later		
12.2ZG	Migrate to 12.3(4)T6 or later		
12.2ZH	Migrate to 12.3(4)T6 or later		
12.2ZI	Migrate to 12.2(18)S or later		
12.2ZJ	Migrate to 12.3 or later		
12.2ZL	Migrate to 12.3(7)T or later		
12.2ZN	Migrate to 12.3(2)T6 or later		

12.2ZO	Migrate to 12.2(15)T12 or later		
12.2ZP	Migrate to 12.3(8)XY or later		
Affected 12.3-Based Release	**Rebuild**	**Interim**	**Maintenance**
12.3	12.3(3f)		
	12.3(5c)		
	12.3(6a)		
			12.3(9)
12.3BC			12.3(9a)BC
12.3B	12.3(5a)B2		
12.3BW	Migrate to 12.3(5a)B2 or later		
12.3JA			12.3(2)JA
12.3T	12.3(2)T6		
	12.3(4)T6		
			12.3(7)T
12.3XA	Migrate to 12.3(7)T or later		

12.3XB	Migrate to 12.3(8)T or later		
12.3XC	Migrate 12.3(2)XC3 or later		
12.3XD	12.3(4)XD4		
12.3XE	12.3(2)XE1		
12.3XF	Migrate to 12.3(11)T or later		
12.3XG	12.3(4)XG2		
12.3XH	Migrate to 12.3(11)T or later		
12.3XI			12.3(7)XI
12.3XJ	12.3(7)XJ		
12.3XK	12.3(4)XK1		
12.3XL			12.3(7)XL
12.3XM			12.3(7)XM
12.3XN	Migrate to 12.3(14)T or later		
12.3XQ	12.3(4)XQ		
12.3XR			12.3(7)XR
12.3XS	12.3(7)XS		

12.3XT	12.3(2)XT		
12.3XU	12.3(8)XU		
12.3XX			12.3(8)XX
12.3XW			12.3(8)XW
12.3XY			12.3(8)XY
12.3XZ			12.3(2)XZ
12.3YA			12.3(8)YA
12.3YD			12.3(8)YD
12.3YE			12.3(4)YE
12.3YF			12.3(11)YF
12.3YG			12.3(8)YG
12.3YH			12.3(8)YH

When considering software upgrades, please also consulthttp://www.cisco.com/en/US/products/products_security_advisories_listing.html and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) for assistance.

Top of the section Close Section

Workarounds

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure access control lists (ACLs) are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists", available at http://www.cisco.com/warp/public/707/iacl.html, presents guidelines and recommended deployment techniques for infrastructure protection ACLs. Exceptions would include any devices which have a legitimate reason to access your infrastructure (for example, BGP peers, DNS servers, and so on). All other traffic must be able to traverse your network without terminating on any of your devices.

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.

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 athttp://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 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.

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

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

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 advisory will be posted on Cisco's worldwide website athttp://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050126-ipv6.

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

- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- comp.dcom.sys.cisco@newsgate.cisco.com
- Various internal Cisco mailing lists

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

Top of the section Close Section

Revision History

Revision 1.0	2005-January-26	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 athttp://www.cisco.com/web/about/security/psirt/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.