

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)[Security Advisories](#)

Cisco Security Advisory: IPv6 Crafted Packet Vulnerability

Revision 1.8

Last Updated 2005 August 11 1800 UTC

For Public Release 2005 July 29 0800 UTC

Please provide your **feedback** on this document.

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Obtaining Fixed Software](#)

[Workarounds](#)

[Exploitation and Public Announcements](#)

[Status of This Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

Cisco Internetwork Operating System (IOS[®]) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

Cisco has made free software available to address this vulnerability for all affected customers.

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>.

Affected Products

Vulnerable Products

This issue affects all Cisco devices running any unfixed version of Cisco IOS or Cisco IOS XR code that supports, and is configured for, IPv6. A system which supports IPv6, if not specifically configured for IPv6, is not affected. You can use the **show ipv6 interface** command to determine whether IPv6 is enabled on a system.

Sample output of the **show ipv6 interface** command is shown below for two systems, one not configured for IPv6 and one configured for IPv6.

An empty output or an error message will be displayed if IPv6 is disabled or unsupported on the system.

```
Router#show ipv6 int fa 0/0
```

-here you see blank output

In the example below the system is vulnerable.

```
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
  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.

Note: Cisco 6500 and 7600 series systems that run 12.2(17a)SX, 12.2(17b)SXA or 12.2(17d)SXB based images automatically enable IPv6 on interfaces where Multi Protocol Label Switching (MPLS) is enabled. MPLS is enabled on an interface by the **mpls ip** or **tag-switching ip** commands. You can use the **show ipv6 interface** command to determine whether IPv6 is enabled on any interface.

To determine the software running on a Cisco product, log in to the device and issue the **show version** command to display the system banner. Cisco IOS Software will identify itself as "Internetwork Operating System Software" or simply "IOS." On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the **show version** command or will give different output.

The following example shows a product running IOS release 12.3(6) with an image name of C2600-JS-

MZ:

```
Cisco Internetwork Operating System Software IOS (tm)  
C2600 Software (C2600-JS-MZ), Version 12.3(6), RELEASE SOFTWARE (fc1)
```

Additional information about Cisco IOS release naming can be found at <http://www.cisco.com/warp/public/620/1.html>.

A system that is running a Cisco IOS XR version prior to 3.2 is also affected by this vulnerability if configured for IPv6. The **show ipv6 interface** command can be used to identify whether IPv6 is enabled on a system running Cisco IOS XR.

Products Confirmed Not Vulnerable

Products that are not running Cisco IOS or Cisco IOS XR 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.

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. Crafted packets from the local segment received on logical interfaces (that is, tunnels including 6to4 tunnels) as well as physical interfaces can trigger this vulnerability. Crafted packets can not traverse a 6to4 tunnel and attack a box across the tunnel.

The crafted packet must be sent from a local network segment to trigger the attack. This vulnerability can not be exploited one or more hops from the IOS device.

This issue is documented in Cisco bug ID [CSCef68324](#) ([registered](#) customers only) for Cisco IOS, and [CSCeh74956](#) ([registered](#) customers only) for Cisco IOS XR.

Impact

Successful exploitation of the vulnerability on Cisco IOS may result in a reload of the device or execution of arbitrary code. Repeated exploitation could result in a sustained DoS attack or execution of arbitrary code on Cisco IOS devices.

Successful exploitation of the vulnerability on Cisco IOS-XR may result in a restart of the IPv6 neighbor discovery process. A restart of this process will only affect IPv6 traffic passing through the system. All other processes and traffic will be unaffected. Repeated exploitation could result in a sustained DoS attack on IPv6 traffic.

Software Versions and Fixes

Each row of the Cisco IOS software table below describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the First Fixed Release) and the anticipated date of availability for each are listed in the Rebuild and Maintenance columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Release	Rebuild	Maintenance
12.0S	12.0(26)S6	
	12.0(27)S5	
	12.0(28)S3	
	12.0(30)S2	12.0(31)S
12.0SL	Vulnerable; migrate to 12.0(31)S or later	
12.0ST	Vulnerable; migrate to 12.0(31)S or later	
12.0SY	Vulnerable; migrate to 12.0(31)S or later	
Affected 12.1-Based Release	Rebuild	Maintenance
12.1XU	Vulnerable; migrate to 12.3(15) or later	
12.1XV	Vulnerable; migrate to 12.3(15) or later	
12.1YB	Vulnerable; migrate to 12.3(15) or later	
12.1YC	Vulnerable; migrate to 12.3(15) or later	
12.1YD	Vulnerable; migrate to 12.3(15) or later	
12.1YE	Vulnerable; migrate to 12.3(15) or later	
12.1YF	Vulnerable; migrate to 12.3(15) or later	
12.1YH	Vulnerable; migrate to 12.3(15) or later	
12.1YI	Vulnerable; migrate to 12.3(15) or later	
Affected 12.2-Based Release	Rebuild	Maintenance
12.2B	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.2BC	12.2(15)BC2h	
12.2BW	Vulnerable; migrate to 12.3(15) or later	
12.2BY	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.2BX	Vulnerable; migrate to 12.3(7)XI4 or later	

12.2BZ	Vulnerable; migrate to 12.3(7)XI4 or later	
12.2CX	Vulnerable; migrate to 12.3(13a)BC or later	
12.2CY	Vulnerable; migrate to 12.3(13a)BC or later	
12.2DD	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.2DX	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.2EU	12.2(20)EU1	
12.2EW	12.2(20)EW2	
12.2EWA	12.2(20)EWA2	
	12.2(25)EWA1	
12.2EZ	12.2(25)EZ1	
12.2JA	Vulnerable; migrate to 12.3(4)JA or later	
12.2JK	12.2(15)JK4	
12.2MB	12.2(4)MB13b	
12.2MC	12.2(15)MC2c	
	12.2(15)MC1c is vulnerable; migrate to 12.4(2)MR	
12.2MX	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.2S	12.2(14)S14	
	12.2(18)S9	
	12.2(20)S8	
	12.2(25)S4	
12.2SEB	12.2(25)SEB3	
12.2SEC	12.2(25)SEC1	
12.2SO	Vulnerable; contact TAC	
12.2SU	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.2SV	12.2(18)SV3, 12.2(22)SV1, 12.2(23)SV1, 12.2(24)SV1, 12.2(25)SV2	12.2(26)SV
12.2SW	12.2(25)SW3a	
12.2SX	Vulnerable; migrate to 12.2(17d)SXB8 or later	

12.2SXA	Vulnerable; migrate to 12.2(17d)SXB8 or later	
12.2SXB	12.2(17d)SXB8	
12.2SXD	12.2(18)SXD4	
12.2SXE	12.2(18)SXE1	
12.2SY	Vulnerable; migrate to 12.2(17d)SXB8 or later	
12.2SZ	Vulnerable; migrate to 12.2(20)S8 or later	
12.2T	12.2(13)T16	
	12.2(15)T16	
12.2XA	Vulnerable; migrate to 12.3(15) or later	
12.2XB	Vulnerable; migrate to 12.3(15) or later	
12.2XC	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.2XD	Vulnerable; migrate to 12.3(15) or later	
12.2XE	Vulnerable; migrate to 12.3(15) or later	
12.2XF	Vulnerable; migrate to 12.3(13a)BC or later	
12.2XG	Vulnerable; migrate to 12.3(15) or later	
12.2XH	Vulnerable; migrate to 12.3(15) or later	
12.2XI	Vulnerable; migrate to 12.3(15) or later	
12.2XJ	Vulnerable; migrate to 12.3(15) or later	
12.2XK	Vulnerable; migrate to 12.3(15) or later	
12.2XL	Vulnerable; migrate to 12.3(15) or later	
12.2XM	Vulnerable; migrate to 12.3(15) or later	
12.2XN	Vulnerable; migrate to 12.3(15) or later	
12.2XQ	Vulnerable; migrate to 12.3(15) or later	
12.2XR	Vulnerable; migrate to 12.3(4)JA or later	
12.2XT	Vulnerable; migrate to 12.3(15) or later	
12.2XU	Vulnerable; migrate to 12.3(15) or later	
12.2XW	Vulnerable; migrate to 12.3(15) or later	
12.2XZ	Vulnerable; migrate to 12.3(15) or later	
12.2YA	12.2(4)YA10	
12.2YB	Vulnerable; migrate to 12.3(15) or later	
12.2YC	Vulnerable; migrate to 12.3(15) or later	

12.2YD	Vulnerable; migrate to fixed 12.3(14)T2 or later
12.2YE	Vulnerable; migrate to 12.2(25)S4 or later
12.2YF	Vulnerable; migrate to 12.3(15) or later
12.2YG	Vulnerable; migrate to 12.3(15) or later
12.2YH	Vulnerable; migrate to 12.3(15) or later
12.2YJ	Vulnerable; migrate to 12.3(15) or later
12.2YK	Vulnerable; migrate to fixed 12.3(14)T2 or later
12.2YL	Vulnerable; migrate to fixed 12.3(14)T2 or later
12.2YM	Vulnerable; migrate to fixed 12.3(14)T2 or later
12.2YN	Vulnerable; migrate to fixed 12.3(14)T2 or later
12.2YO	Vulnerable; migrate to 12.2(17d)SXB8 or later
12.2YP	Vulnerable; migrate to 12.3(15) or later
12.2YQ	Vulnerable; migrate to fixed 12.3(14)T2 or later
12.2YR	Vulnerable; migrate to fixed 12.3(14)T2 or later
12.2YT	Vulnerable; migrate to 12.2(15)T16 or later
12.2YU	Vulnerable; migrate to fixed 12.3(14)T2 or later
12.2YV	Vulnerable; migrate to fixed 12.3(14)T2 or later
12.2YW	Vulnerable; migrate to fixed 12.3(14)T2 or later
12.2YX	Vulnerable; migrate to fixed 12.3(14)T2 or later
12.2YY	Vulnerable; migrate to fixed 12.3(14)T2 or later
12.2YZ	Vulnerable; migrate to 12.2(20)S8 or later
12.2ZA	Vulnerable; migrate to 12.2(17d)SXB8 or later
12.2ZB	Vulnerable; migrate to fixed 12.3(14)T2 or later

12.2ZC	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.2ZD	12.2(13)ZD3	
12.2ZE	Vulnerable; migrate to 12.3(15) or later	
12.2ZF	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.2ZG	Vulnerable; contact TAC	
12.2ZH	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.2ZJ	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.2ZL	Vulnerable; contact TAC	
12.2ZN	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.2ZO	Vulnerable; migrate to 12.2(15)T16 or later	
12.2ZP	Vulnerable; migrate to 12.3(8)XY6 or later	
Affected 12.3-Based Release	Rebuild	Maintenance
12.3	12.3(3h)	
	12.3(5e)	
	12.3(6e)	
	12.3(9d)	
	12.3(10d)	
	12.3(12b)	
	12.3(13a)	12.3(15)
12.3B	12.3(5a)B5	
12.3BC	12.3(9a)BC6	12.3(13a)BC
12.3BW	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.3JA		12.3(4)JA
12.3JK		12.3(2)JK
12.3T	12.3(7)T9	
	12.3(8)T8	
	12.3(11)T5	
	12.3(14)T2	

12.3XA	12.3(2)XA4	
12.3XB	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.3XC	12.3(2)XC3	
12.3XD	Vulnerable; contact TAC	
12.3XE	12.3(2)XE3	
12.3XF	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.3XG	12.3(4)XG4	
12.3XH	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.3XI	12.3(7)XI4	
12.3XJ	Vulnerable; migrate to 12.3(11)YF3 or later	
12.3XK	12.3(4)XK3	
12.3XL	Vulnerable; contact TAC	
12.3XM	Vulnerable; migrate to fixed 12.3(14)T2 or later	
12.3XQ	12.3(4)XQ1	
12.3XR	12.3(7)XR4	
12.3XS	Vulnerable; migrate to 12.4(1) or later	
12.3XT	Vulnerable; contact TAC	
12.3XU	Vulnerable; migrate to 12.4(2)T or later	
12.3XW	Vulnerable; migrate to 12.3(11)YF3 or later	
12.3XX	Vulnerable; migrate to 12.4(1) or later	
12.3XY	12.3(8)XY6	
12.3YA	12.3(8)YA1	
12.3YD	Vulnerable; migrate to 12.4(2)T	
12.3YF	12.3(11)YF3	
12.3YG	12.3(8)YG2	
12.3YH	Vulnerable; migrate to 12.3(8)YI1 or later	
12.3YI	12.3(8)YI1	
12.3YJ	12.3(11)YJ	
12.3YK	Vulnerable; contact TAC	
12.3YQ	12.3(14)YQ1	

12.3YS		12.3(11)YS
12.3YT		12.3(14)YT
12.3YU		12.3(14)YU
Affected 12.4- Based Release	Rebuild	Maintenance
12.4		12.4(1)
12.4MR		12.4(2)MR
12.4T		12.4(2)T

Product	First Fixed Release
Cisco IOS XR	IOS XR 3.2
	Contact TAC to obtain SMU AA01233 for IOS XR 3.0.1.
	Contact TAC to obtain SMU AA01234 for IOS XR 3.1.0.

For further information on the terms "Rebuild" and "Maintenance, " please consult the following URL:
<http://www.cisco.com/warp/public/620/1.html>

When considering software upgrades, please also consult http://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.

Obtaining Fixed Software

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 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 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

Please 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.

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

See <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.

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>.

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.

In networks where IPv6 is not needed but enabled, disabling IPv6 processing on an IOS device will eliminate exposure to this vulnerability. On a router which is configured for IPv6, this must be done by issuing the command **no ipv6 enable** and **no ipv6 address** on each interface.

Exploitation and Public Announcements

This vulnerability was disclosed on July 27, 2005 at the Black Hat security conference.

Status of This Notice: FINAL

THIS ADVISORY IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE ADVISORY OR MATERIALS LINKED FROM THE ADVISORY IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR

UPDATE THIS NOTICE AT ANY TIME.

A stand-alone copy or paraphrase of the text of this security advisory 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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.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
- 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.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

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.

Revision History

Revision 1.8	2005-August-11	Status changed from Interim to Final.
Revision 1.7	2005-August-05	Software Versions and Fixes table updated for Cisco IOS XR.
Revision 1.6	2005-August-03	Added a note to the Affected Products section. Software Versions and Fixes table updated for 12.2EZ.
Revision 1.5	2005-August-02	Software Versions and Fixes table updated for 12.2JK, 12.2MC, 12.2ZD, 12.3XA, 12.3XE, 12.3XG, and 12.3XK; removed 12.2CZ.
Revision 1.4	2005-August-01	Software Versions and Fixes table updated for 12.2BC, 12.2EZ, 12.2SEB, and 12.2SW.
Revision	2005-	Software Versions and Fixes table

1.3	July-31	updated.
Revision 1.2	2005- July-30	IOS XR added to Affected Products. Wording changes made in the Workarounds section. Software Versions and Fixes table updated.
Revision 1.1	2005- July-29	Software Versions and Fixes table updated. First paragraph in the Vulnerable Products section updated.
Revision 1.0	2005- July-29	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>.

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 1992-2005 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).