

Cisco Security Advisory: Cisco IOS Malformed BGP Packet Causes Reload

Document ID: 53021

Advisory ID: cisco-sa-20040616-bgp

<http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>

Revision 1.1

Last Updated 2006 January 12 1930 UTC (GMT)

For Public Release 2004 June 16 1500 UTC (GMT)

Please provide your [feedback](#) on this document.

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of This Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

Cisco has made free software available to address this problem.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

This issue affects all Cisco devices running any unfixed version of Cisco IOS or Cisco IOS XR code and configured for BGP routing.

A router which is running the BGP process will have a line in the config defining the AS number, which can be seen by issuing the command `show running-config`:

```
router bgp <AS number>
```

This vulnerability is present in any unfixed version of IOS, from the beginning of support for the BGP protocol, including versions 9.x, 10.x, 11.x and 12.x.

This vulnerability is present in any unfixed version of IOS XR, from the beginning of support for the BGP protocol, including versions 2.0.X and 3.0.X

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 identifies a Cisco product running IOS release 12.0(3) with an installed image name of C2500-IS-L:

```
Cisco Internetwork Operating System Software IOS (TM)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

The release train label is "12.0."

The next example shows a product running IOS release 12.0(2a)T1 with an image name of C2600-JS-MZ:

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

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

Products Confirmed Not Vulnerable

Products confirmed not to be vulnerable include devices which cannot participate in BGP or cannot be configured for BGP.

Details

The Border Gateway Protocol (BGP) is a routing protocol defined by RFC 1771, and designed to manage IP routing in large networks. An affected Cisco device running a vulnerable version of Cisco IOS software and enabling the BGP protocol will reload when a malformed BGP packet is received. BGP runs over TCP, a reliable transport protocol which requires a valid three way handshake before any further messages will be accepted. The Cisco IOS implementation of BGP requires the explicit definition of a neighbor before a connection can be established, and traffic must appear to come from that neighbor. These implementation details make it very difficult to send a BGP packet to a Cisco IOS device from an unauthorized source.

A Cisco device receiving an invalid BGP packet will reset and may take several minutes to become fully functional. This vulnerability may be exploited repeatedly resulting in an extended DOS attack. This issue is documented in bug IDs [CSCdu53656](#) ([registered](#) customers only) and [CSCea28131](#) ([registered](#) customers only) .

Impact

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

Software Versions and Fixes

Note: Many of the releases in this table were fixed prior to the release of other IOS advisories. Read the table carefully to determine if your IOS release contains these fixes. Most fixed releases for the TCP and SNMP advisories such as <http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml> and <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml> contained the fixes for this BGP advisory.

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," "Interim," 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). When selecting a release, keep in mind the following definitions:

Maintenance

Most heavily tested, stable, and highly recommended release of a release train in any given row of the table.

Rebuild

Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific defect. Although it receives less testing, it contains only the minimal changes necessary to repair the vulnerability.

Interim

Built at regular intervals between maintenance releases and receives less testing. Interims should be selected only if there is no other suitable release that addresses the vulnerability. Interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available through manufacturing, and usually they are not available for customer download from Cisco.com without prior arrangement with the Cisco TAC.

In all cases, customers should exercise caution to confirm that the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new software release. If the information is not clear, contact the Cisco TAC for assistance as shown in the [Obtaining Fixed Software](#) section below.

More information on Cisco IOS software release names and abbreviations is available at <http://www.cisco.com/warp/public/620/1.html>.

The fixes will be available at the Software Center located at <http://www.cisco.com/tacpage/sw-center/>.

For software installation and upgrade procedures, see http://www.cisco.com/warp/public/130/upgrade_index.shtml.

For a current view of all posted and repaired images for Cisco IOS, please check the listing available to registered Cisco.com users at: <http://www.cisco.com/tacpage/sw-center/sw-ios.shtml>.

Major Release	Availability of Repaired Releases*		
Affected 11.1-Based Release	Rebuild	Interim**	Maintenance
11.1	Migrate to 11.2 or later		
11.1AA	Migrate to 11.2P or later		
11.1CA	Migrate to 12.0 or later		
11.1CC	Migrate to 12.0 or later		
Affected 11.2-Based Release	Rebuild	Interim**	Maintenance
11.2	11.2(26g)		
11.2P	11.2(26)P7		
11.2SA	Not Vulnerable		
Affected 11.3-Based Release	Rebuild	Interim**	Maintenance
11.3	11.3(11f)		
11.3T	11.3(11b)T5		
Affected 12.0-Based Release	Rebuild	Interim**	Maintenance
12.0			12.0(27)
12.0DA	Migrate to 12.2DA or later		
12.0S	12.0(21)S7		
	12.0(22)S2e		
	12.0(22)S3c		
	12.0(22)S4a		
	12.0(22)S5		
	12.0(23)S3		
	12.0(24)S2		
	12.0(25)S1		
			12.0(26)S
12.0SL	Migrate to 12.0(23)S3 or later		
12.0ST	12.0(17)ST10 Available upon request		

	12.0(21)ST7		
	Migrate to 12.0(26)S2 or later		
12.0SV			12.0(27)SV
12.0SX	12.0(25)SX		
12.0SZ	12.0(23)SZ3		
			12.0(26)SZ
	Migrate to 12.0(26)S2 or later		
12.0T	Migrate to 12.1 or later		
12.0W5	12.0(16)W5(21c)		
	12.0(25)W5(27b)		
	12.0(26)W5(28a)		
	12.0(27)W5(29)		
12.0WC	Not Vulnerable		
12.0WX	Migrate to 12.0W5 or later		
12.0XA	Migrate to 12.1 latest or later		
12.0XC	Migrate to 12.1 latest or later		
12.0XD	Migrate to 12.1 latest or later		
12.0XE	Migrate to 12.1E latest or later		
12.0XG	Migrate to 12.1 latest or later		
12.0XH	Migrate to 12.1 latest or later		
12.0XI	Migrate to 12.1 latest or later		
12.0XJ	Migrate to 12.1 latest or later		
12.0XK	Migrate to 12.1T latest or later		
12.0XL	Migrate to 12.2 latest or later		
12.0XN	Migrate to 12.1 latest or later		
12.0XP	Not Vulnerable		
12.0XR	Migrate to 12.2 latest or later		
12.0XS	Migrate to 12.1E latest or later		
12.0XU	Not Vulnerable		
Affected 12.1–Based Release	Rebuild	Interim**	Maintenance
12.1			12.1(20)
12.1AA	Migrate to 12.2 latest or later		
12.1AX	Not Vulnerable		
	12.1AY	Not Vulnerable	
12.1AZ			12.1(14)AZ

12.1DA	Migrate to 12.2DA or later		
12.1DB	Migrate to 12.2B or later		
12.1E	12.1(6)E12.0		
	12.1(8b)E14		
	12.1(11b)E12.0		
	12.1(12c)E7		
	12.1(13)E6		
	12.1(14)E4		
	12.1(19)E		
			12.1(20)E
12.1EA	12.1(14)EA1		
12.1EB	12.1(14)EB1		
12.1EC			12.1(19)EC
12.1EO			12.1(19)EO
12.1EV	12.1(12c)EV2		
12.1EW			12.1(19)EW
12.1EX	Migrate to 12.1(14)E4 or later		
12.1EY	Migrate to 12.1(14)E4 or later		
12.1T	12.1(5)T19		
12.1XA	Migrate to 12.1(5)T19 or later		
12.1XB	Migrate to 12.1(5)T19 or later		
12.1XC	Migrate to 12.1(5)T19 or later		
12.1XD	Migrate to 12.2 or later		
12.1XE	Migrate to 12.1E latest or later		
12.1XF	Migrate to 12.2(4)T6 or later		
12.1XG	Migrate to 12.2(4)T6 or later		
12.1XH	Migrate to 12.2 or later		
12.1XI	Migrate to 12.2 latest or later		
12.1XJ	Migrate to 12.2(4)T6 or later		
12.1XL	Migrate to 12.2T latest or later		
12.1XM	Migrate to 12.2T latest or later		
12.1XP	Migrate to 12.2(4)T6 or later		
12.1XQ	Migrate to 12.2T latest or later		
12.1XR	Migrate to 12.2T latest or later		
12.1XT	Migrate to 12.2(4)T6 or later		
12.1XU	Migrate to 12.2T latest or later		

12.1XV	Migrate to 12.2XB or later		
12.1XY	Migrate to 12.2XB or later		
12.1YA	Migrate to 12.2(8)T10 or later		
12.1YB	Migrate to 12.2(4)T6 or later		
12.1YC	Migrate to 12.2(8)T10 or later		
12.1YD	Migrate to 12.2(8)T10 or later		
12.1YH	Migrate to 12.2(13)T5 or later		
12.1YJ	Not Vulnerable		
Affected 12.2-Based Release	Rebuild	Interim**	Maintenance
12.2	12.2(10d)		
	12.2(12e)		
	12.2(12h)M1		
	12.2(13c)		
	12.2(16a)		
			12.2(17)
12.2B	12.2(15)B1		
12.2BC	12.2(15)BC1		
12.2BW	Migrate to 12.2(15)T12 or later		
12.2BX			12.2(16)BX
12.2BY	Migrate to 12.2(15)B1 or later		
12.2BZ	Migrate to 12.2(16)BX or later		
12.2CX			12.2(15)CX
12.2DA	12.2(12)DA6		
12.2DD	Migrate to 12.2(15)B1 or later		
12.2DX	Migrate to 12.2(15)B1 or later		
12.2EW			12.2(18)EW
12.2JA			12.2(13)JA
12.2S	12.2(14)S2		
			12.2(18)S
12.2SE			12.2(18)SE
12.2SU			12.2(14)SU
12.2SV			12.2(18)SV
12.2SW			12.2(18)SW
12.2SX	12.2(14)SX2		
12.2SXA	12.2(17b)SXA		

12.2SXB	12.2(17d)SXB		
12.2SY			12.2(14)SY
12.2SZ	12.2(14)SZ2		
12.2T	12.2(4)T6		
	12.2(8)T10		
	12.2(11)T9		
	12.2(13)T5		
	12.2(15)T4		
12.2XA	Migrate to 12.2(11)T9 or later		
12.2XB	12.2(2)XB16		
12.2XD	Migrate to 12.2(8)T10 or later		
12.2XE	Migrate to 12.2(8)T10 or later		
12.2XG	Migrate to 12.2(8)T10 or later		
12.2XH	Migrate to 12.2(11)T9 or later		
12.2XI	Migrate to 12.2(11)T9 or later		
12.2XJ	Migrate to 12.2(11)T9 or later		
12.2XK	Migrate to 12.2(11)T9 or later		
12.2XL	Migrate to 12.2(15)T4 or later		
12.2XM	Migrate to 12.2(15)T4 or later		
12.2XN	Migrate to 12.2(11)T9 or later		
12.2XQ	Migrate to 12.2(11)T9 or later		
12.2XS	Migrate to 12.2(11)T9 or later		
12.2XT	Migrate to 12.2(11)T9 or later		
12.2XU	Migrate to 12.2(15)T12 or later		
12.2XW	Migrate to 12.2(11)T9 or later		
12.2YA	Migrate to 12.2(15)T4 or later		
12.2YB	Migrate to 12.2(15)T4 or later		
12.2YC	Migrate to 12.2(11)T11 or later		
12.2YD	Migrate to 12.2(8)YY or later		
12.2YE	Migrate to 12.2S or later		
12.2YF	Migrate to 12.2(15)T4 or later		
12.2YG	Migrate to 12.2(13)T5 or later		
12.2YH	Migrate to 12.2(15)T4 or later		
12.2YJ	Migrate to 12.2(15)T4 or later		
12.2YL	Migrate to 12.3(2)T or later		
12.2YM	Migrate to 12.3(2)T or later		

12.2YN	Migrate to 12.3(2)T or later		
12.2YO	Migrate to 12.2(14)SY or later		
12.2YP	12.2(11)YP1		
12.2YQ	Migrate to 12.3(4)T or later		
12.2YR	Migrate to 12.3(4)T or later		
12.2YS	Migrate to 12.3T or later		
12.2YT	Migrate to 12.2(15)T4 or later		
12.2YU	Migrate to 12.3(4)T or later		
12.2YV	Migrate to 12.3(4)T or later		
12.2YW	Migrate to 12.3(2)T or later		
12.2YX	Migrate to 12.2(14)SU or later		
12.2YY	12.2(8)YY3		
12.2YZ	Migrate to 12.2(14)SZ or later		
12.2ZA	12.2(14)ZA2		
12.2ZB	Migrate to 12.3T or later		
12.2ZC	Migrate to 12.3T or later		
12.2ZE	Migrate to 12.3 or later		
12.2ZF	Migrate to 12.3(4)T or later		
12.2ZG	Migrate to 12.3(4)T or later		
12.2ZH	Migrate to 12.3(4)T or later		
12.2ZI	Migrate to 12.2(18)S or later		
12.2ZK			12.2(15)ZK
12.2ZL			12.2(15)ZL
12.2ZN	Migrate to 12.3(2)T or later		
12.2ZO			12.2(15)ZO
12.2ZP			12.2(13)ZP
Affected 12.3-Based Release	Rebuild	Interim**	Maintenance
12.3	Not Vulnerable		
12.3T	Not Vulnerable		

Product	First Fixed Release
Cisco IOS XR	IOS XR 3.2.5

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.

For additional information regarding BGP security risk assessment, mitigation techniques, and deployment best practices, please consult <ftp://ftp-eng.cisco.com/cons/isp/security/BGP-Risk-Assesment-v.pdf>.

BGP MD5

Under normal circumstances, due to inherent security factors in the TCP protocol such as sequence number checks, it is difficult but possible to forge an appropriate packet to exploit this problem. Configuring your Cisco IOS device for BGP MD5 authentication is a valid workaround to protect the vulnerable device.

This can be configured as shown in the following example:

```
router(config)# router bgp
router(config-router)# neighbor <IP_address> password <enter_your_secret_here>
```

It is necessary to configure the same shared MD5 secret on both peers and at the same time. Failure to do so will break the existing BGP session and the new session will not get established until the exact same secret is configured on both devices. For a detailed discussion on how to configure BGP, refer to the following document:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a00800ca5711

Once the secret is configured, it is prudent to change it periodically. The exact period must fit within your company security policy but it should not be longer than a few months. When changing the secret, again it must be done at the same time on both devices. Failure to do so will break your existing BGP session. The exception is if your Cisco IOS software release contains the integrated [CSCdx23494](#) ([registered](#) customers only) fix **on both sides of the connection**. With this fix, the BGP session will not be terminated when the MD5 secret is changed only on one side. The BGP updates, however, will not be processed until either the same secret is configured on both devices or the secret is removed from both devices.

Infrastructure Access Control Lists

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 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" presents guidelines and recommended deployment techniques for infrastructure protection ACLs:

<http://www.cisco.com/warp/public/707/iacl.html>

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 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 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.

Exploitation and Public Announcements

The research which led to this vulnerability being discovered was announced in a public announcement at NANOG in June 2003. The Cisco PSIRT team is not aware of any malicious use of the vulnerabilities described in this advisory. We were made aware of this issue through internal testing as well as notification from a research team at the University of California at Santa Barbara.

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

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.

Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.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.netsys.com
- 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 1.1	12-January-2006	Updated the Vulnerable Products section. Added the Products/First Fixed Release table to the Software Versions and Fixes section.
Revision 1.0	16-June-2004	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>.
