

Cisco Security Advisory: Cisco IOS BGP Attribute Corruption Vulnerability

Document ID: 10935

Advisory ID: cisco-sa-20010510-ios-bgp-attr

<http://www.cisco.com/warp/public/707/cisco-sa-20010510-ios-bgp-attr.shtml>

Revision 1.1

Last Updated 2001 November 29 1500 UTC (GMT)

For Public Release 2001 May 10 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 Border Gateway Protocol (BGP) UPDATE contains Network Layer Reachability Information (NLRI) and attributes that describe the path to the destination. An unrecognized transitive attribute can cause failures in Cisco IOS routers, ranging from a crash upon receipt of the unrecognized transitive attribute, to a later failure upon attempt to clear the unrecognized transitive attribute. Specific but common configurations are affected, and described below. The failure was discovered because of a malfunction in the BGP implementation of another vendor. There is no workaround. Affected customers are urged to upgrade to fixed code.

This vulnerability has been assigned Cisco bug ID CSCdt79947.

The complete text of this advisory will be located at
<http://www.cisco.com/warp/public/707/cisco-sa-20010510-ios-bgp-attr.shtml>

Affected Products

Vulnerable Products

Configurations including BGP4 Prefix Filtering with Inbound Route Maps are vulnerable. BGP with prefix inbound routemap filtering was introduced in Cisco IOS® Software version 11.2. The following versions of Cisco IOS Software are affected and listed in the table below: 11.CC and its derivatives, 11.2 and its derivatives, 11.3, 11.3T, 12.0, 12.0S and special branches taken out of 12.0 are all affected. The versions of Cisco IOS Software based on 12.1, 12.0(5)T, 12.2, 12.0ST, and 12.1(E) are *not* affected. The following products are affected if they run a Cisco IOS software release that has the defect. To determine if a Cisco product is running an affected IOS, log in to the device and issue the **show version** command. Cisco IOS software will identify itself as "Internetwork Operating System Software" or "IOS (tm)" software and will display a version number. Other Cisco devices either will not have the **show version** command, or will give different output. Compare the version number obtained from the router with the versions presented in the Software Versions and Fixes section below.

Cisco devices that may be running with affected Cisco IOS software releases include:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800, ubr900, 1000, 1400, 1500, 1600, 1700, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200, ubr7200, 7500, and 12000 series.

Products Confirmed Not Vulnerable

Cisco devices that may be running Cisco IOS Software, but do NOT support BGP and are therefore not vulnerable include:

- Most recent versions of the LS1010 ATM switch.
- The Catalyst 2900XL LAN switch only if it is running IOS.
- The Catalyst 1900, 2800, 2900, 3000, and 5000 series LAN switches.
- The Cisco DistributedDirector.

If you are not running Cisco IOS software, you are not affected by this vulnerability. If you are not running BGP, you are not affected by this vulnerability.

Cisco products that do not run Cisco IOS software and are not affected by this defect include, but are not limited to:

- 700 series dialup routers (750, 760, and 770 series) are not affected.
- The Catalyst 6000 is not affected if it is not running IOS.
- WAN switching products in the IGX and BPX lines are not affected.
- The MGX (formerly known as the AXIS shelf) is not affected.
- No host-based software is affected.
- The Cisco PIX Firewall is not affected.
- The Cisco LocalDirector is not affected.
- The Cisco Cache Engine is not affected.

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

Details

A Border Gateway Protocol (BGP) UPDATE contains Network Layer Reachability Information (NLRI) and attributes that describe the path to the destination. Each path attribute is a type, length, value (TLV) object.

Cisco Security Advisory: Cisco IOS BGP Attribute Corruption Vulnerability

This failure occurs as a result of memory corruption and only in configurations using specific inbound route filtering. The failure was discovered because of a malfunction in the BGP implementation of another vendor. There is no workaround.

Impact

The vulnerability can be exercised repeatedly, affecting core routers, creating widespread network outages. This vulnerability can only be exercised in configurations that include both BGP and inbound route filtering on affected software.

Software Versions and Fixes

The following table summarizes the Cisco IOS software releases that are known to be affected, and the earliest estimated dates of availability for the recommended fixed versions. **Dates are always tentative and subject to change.**

Each row of the table 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 and the anticipated date of availability for each are listed in the "Rebuild", "Interim", and "Maintenance" columns. A device running any release in the given train that is earlier than the release in a specific column (less than the earliest fixed release) is known to be vulnerable, and it should be upgraded at least to the indicated release or a later version (greater than the earliest fixed release label).

When selecting a release, keep in mind the following definitions:

- **Maintenance**
Most heavily tested and highly recommended release of any label in a 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 effect the repair.
- **Interim**
Built at regular intervals between maintenance releases and receive less testing. Interims should be selected only if there is no other suitable release that addresses the vulnerability, and interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available via manufacturing, and usually they are not available for customer download from CCO without prior arrangement with the Cisco TAC.

In the table below, the logical superseding software is recommended when there is no rebuild or maintenance planned for a specific software release. Customers should verify that planned upgrades will meet their requirements. For further details, see the IOS Release Notes for each Cisco IOS Train.

<http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm>. 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 TAC for assistance as shown later in this notice.

More information on Cisco IOS Software release names and abbreviations is available at http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html.

Train	Description of Image or Platform	Availability of Fixed Releases*
-------	----------------------------------	---------------------------------

11.0-based Releases		Rebuild	Interim	Maintenance
11.0	Major GD release for all platforms	Not vulnerable		
11.1-based Releases		Rebuild	Interim	Maintenance
11.1	Major release for all platforms	Not vulnerable		
11.1AA	ED release for access servers: 1600, 3200, and 5200 series.	Not vulnerable		
11.1CA	Platform-specific support for 7500, 7200, 7000, and RSP	End of Engineering		
11.1CC	ISP train: added support for FIB, CEF, and NetFlow on 7500, 7200, 7000, and RSP	Not scheduled 11.1(36)CC2		
11.1CT	Added support for Tag Switching on 7500, 7200, 7000, and RSP	2001-May-29 End of Engineering		
11.1IA	Distributed Director only	Upgrade recommended to 12.0ST Not Vulnerable		
11.2-based Releases		Rebuild	Interim	Maintenance
11.2	Major release, general deployment	End of Engineering		
11.2BC	Platform-specific support for IBM networking, CIP, and TN3270 on 7500, 7000, and RSP	Not scheduled End of Engineering		
11.2F	Feature train for all platforms	Upgrade recommended to 12.1(8) End of Engineering		
11.2GS	Early deployment release to support 12000 GSR	Upgrade recommended End of Engineering		
11.2P	New platform support	Upgrade recommended to 12.0(17)S End of Engineering		
11.2SA	Catalyst 2900XL switch only	Upgrade recommended to 12.0(17) Not vulnerable		

11.2WA3	LightStream 1010 ATM switch	Not vulnerable
11.2(4)XA	Initial release for the 1600 and 3600	End of Engineering
		Upgrade recommended
11.2(9)XA	Initial release for the 5300 and digital modem support for the 3600	End of Engineering
11.3-based Releases		Upgrade recommended
		Rebuild Interim Maintenance
11.3	Major release for all platforms	End of Engineering
		Upgrade recommended to 12.0(17)
11.3AA	ED for dial platforms and access servers: 5800, 5200, 5300, 7200	End of Engineering
		Upgrade recommended to 12.0(17)
11.3DA	Early deployment train for ISP DSLAM 6200 platform	End of Engineering
		Upgrade recommended to 12.1DA
11.3DB	Early deployment train for ISP/Telco/PTT xDSL broadband concentrator platform, (NRP) for 6400	End of Engineering
		Upgrade recommended to 12.1DB
11.3HA	Short-lived ED release for ISR 3300 (SONET/SDH router)	End of Engineering
		Upgrade recommended to 12.0
11.3MA	MC3810 functionality only	Not available
		Not scheduled
11.3NA	Voice over IP, media convergence, various platforms	End of Engineering
		Upgrade recommended to 12.1
11.3T	Early deployment major release, feature-rich for early adopters	End of Engineering
		Upgrade recommended to 12.0(17)
11.3WA4	Multilayer Switching and	End of Engineering

	Multiprotocol over ATM functionality for Catalyst 5000 RSM, 4500, 4700, 7200, 7500, LightStream 1010	Upgrade recommended		
11.3(2)XA	Introduction ofubr7246 and 2600	End of Engineering		
12.0-based Releases		Upgrade recommended		
		Rebuild	Interim	Maintenance
12.0	General deployment release for all platforms			12.0(17) 2001-Apr-23
12.0DA	xDSL support: 6100, 6200	Unavailable		
		Upgrade recommended to 12.1DA		
12.0DB	Early Deployment (ED) release, which delivers support for the Cisco 6400 Universal Access Concentrator (UAC) for Node Switch Processor (NSP)	Unavailable		
		Upgrade recommended to 12.1DB		
12.0DC	Early Deployment (ED) release, which delivers support for the Cisco 6400 Universal Access Concentrator (UAC) for Node Route Processor (NRP)	Unavailable		
		Upgrade recommended to 12.1DC		
12.0S	Core/ISP support: GSR, RSP, c7200	12.0(15)S3, 12.0(16)S1 2001-April-23 2001-April-30	12.0(16.06)S 2001-May-07	12.0(17)S 2001-May-07
12.0SC	Cable/broadband ISP: ubr7200	Not vulnerable		
12.0SL	10000 ESR: c10k	Not vulnerable		
12.0ST	Cisco IOS software Release 12.0ST is	Not vulnerable		

	an early deployment (ED) release for the Cisco 7200, 7500/7000RSP and 12000 (GSR) series routers for Service Providers (ISPs).			
12.0T	Early Deployment(ED): VPN, Distributed Director, various platforms			12.0(5)T
12.0W5	Catalyst switches: cat2948g-13, cat4232	12.0(10)W5(18g)		
	cat8510c, cat8540c, c6msm, ls1010, cat8510m, cat8540m, c5atm	2001-Apr-20		12.0(16)W5(21)
12.0WT	Catalyst switches: cat4840g	2001-May-21 Not vulnerable		
12.0XA	Early Deployment (ED): limited platforms	Unavailable		
12.0XB	Short-lived early deployment release	Upgrade recommended to 12.1 Unavailable		
12.0XC	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1 Unavailable		
12.0XD	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1 Unavailable		
12.0XE	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1 Not Vulnerable		
12.0XF	Early Deployment (ED): limited platforms	Unavailable		
12.0XG	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1 Unavailable		
12.0XH	Early Deployment (ED): limited	Upgrade recommended to 12.1 Unavailable		
		Upgrade recommended to 12.1		

	platforms	
12.0XI	Early Deployment (ED): limited platforms	Unavailable
12.0XJ	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1 Unavailable
12.0XK	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1 Not vulnerable
12.0XL	Early Deployment (ED): limited platforms	Not vulnerable
12.0XM	Short-lived early deployment release	Not vulnerable
12.0XN	Early Deployment (ED): limited platforms	Not vulnerable
12.0XP	Early Deployment (ED): limited platforms	Not vulnerable
12.0XQ	Short-lived early deployment release	Not vulnerable
12.0XR	Short-lived early deployment release	Not vulnerable
12.0XS	Short-lived early deployment release	Not vulnerable
12.0XU	Early Deployment (ED): limited platforms	Not vulnerable
12.0XV	Short-lived early deployment release	Not vulnerable
12.1-based and Later Releases		Rebuild Interim Maintenance
12.1	General deployment release for all platforms	Not vulnerable
Notes		
* All dates are estimated and subject to change.		

** Interim releases are subjected to less rigorous testing than regular maintenance releases, and may have serious bugs.

Workarounds

There are no known workarounds for this vulnerability. Please upgrade to fixed versions.

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

Cisco has had no reports of malicious exploitation of this vulnerability. The failure was discovered because of a malfunction in the BGP implementation of another vendor, which caused a series of crashes that led to the identification of this issue.

Cisco knows of no public announcements of this vulnerability before the date of this notice.

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 notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20010510-ios-bgp-attr.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
- bugtraq@securityfocus.com
- firewalls@lists.gnac.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's Worldwide Web server, 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	2001-November-29	Made changes to upgrade recommendations for some
-----------------	------------------	--

		IOS versions
Revision 1.0	2001–May–10	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 Web site at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jun 14, 2007

Document ID: 10935
