

Cisco Security Advisory: Cisco IOS Software Border Gateway Protocol 4-Byte Autonomous System Number Vulnerabilities

Advisory ID: [cisco-sa-20090729-bgp](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20090729-bgp.shtml>

Revision 1.2

Last Updated 2009 August 3 1300 UTC (GMT)

For Public Release 2009 July 29 1600 UTC (GMT)

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

Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Vulnerability Scoring 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

Recent versions of Cisco IOS Software support RFC4893 ("BGP Support for Four-octet AS Number Space") and contain two remote denial of service (DoS) vulnerabilities when handling specific Border

Gateway Protocol (BGP) updates.

These vulnerabilities affect only devices running Cisco IOS Software with support for four-octet AS number space (here after referred to as 4-byte AS number) and BGP routing configured.

The first vulnerability could cause an affected device to reload when processing a BGP update that contains autonomous system (AS) path segments made up of more than one thousand autonomous systems.

The second vulnerability could cause an affected device to reload when the affected device processes a malformed BGP update that has been crafted to trigger the issue.

Cisco has released free software updates to address these vulnerabilities.

No workarounds are available for the first vulnerability.

A workaround is available for the second vulnerability.

This advisory is posted at the following link: <http://www.cisco.com/warp/public/707/cisco-sa-20090729-bgp.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

These vulnerabilities affect only devices running Cisco IOS and Cisco IOS XE Software (here after both referred to as simply Cisco IOS) with support for RFC4893 and that have been configured for BGP routing.

BGP is configured in Cisco IOS Software with the configuration command **router bgp** *[AS Number]* . The device is vulnerable if it is running affected Cisco IOS version and has BGP configured, regardless of whether the device is configured with a 2 or 4 byte AS number under the **router bgp** configuration command.

The software table in the section "Software Versions and Fixes" of this advisory indicates all affected Cisco IOS Software versions that have support for RFC4893 and are affected by this vulnerability.

A Cisco IOS software version that has support for RFC4893 will allow configuration of AS numbers using 4 Bytes. The following example identifies a Cisco device that has 4 byte AS number support:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp ?
  <1-65535>      Autonomous system number
  <1.0-XX.YY>   4 Octets Autonomous system number
```


Or:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp ?
  <1-4294967295>  Autonomous system number
  <1.0-XX.YY>    Autonomous system number
```

The following example identifies a Cisco device that has 2 byte AS number support:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp ?
  <1-65535>  Autonomous system number
```

A router that is running the BGP process will contain a line in the configuration that defines the autonomous system number (AS number), which can be seen by issuing the command line interface (CLI) command "**show running-config**".

The canonical textual representation of four byte AS Numbers is standardized by the IETF through [RFC5396](#)  (Textual Representation of Autonomous System (AS) Numbers). Two major ways for textual representation have been defined as ASDOT and ASPLAIN. Cisco IOS routers support both textual representations of AS numbers. For further information about textual representation of four byte AS numbers in Cisco IOS Software consult the document "Explaining 4-Byte Autonomous System (AS) ASPLAIN and ASDOT Notation for Cisco IOS" at the following link:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6554/ps6599/white_paper_c11_5

Cisco IOS Software with support for RFC4893 is affected by both vulnerabilities if BGP routing is configured using either ASPLAIN or ASDOT notation, regardless if the AS Number is a 2 byte or 4 byte number.

The following example identifies a Cisco device that is configured for BGP using ASPLAIN notation:

```
router bgp 65536
```

The following example identifies a Cisco device that is configured for BGP using ASDOT notation:

```
router bgp 1.0
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the show version command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the show version command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih
```

!--- output truncated

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.4(20)T with an installed image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
```

!--- output truncated

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link:

<http://www.cisco.com/warp/public/620/1.html>

☐ Products Confirmed Not Vulnerable



The following Cisco products are confirmed not vulnerable:

- Cisco IOS Software not explicitly mentioned in this Advisory
- Cisco IOS XR Software
- Cisco IOS NX-OS

No other Cisco products are currently known to be affected by this vulnerability.

[Top of the section](#) [Close Section](#)

☐ Details

[RFC4271](#)  has defined an AS number as a two-octet entity in BGP. [RFC4893](#)  has defined an AS number as a four-octet entity in BGP.

The first vulnerability could cause an affected device to reload when processing a BGP update that contains AS path segments made up of more than one thousand autonomous systems. If an affected 4-byte AS number BGP speaker receives a BGP update from a 2-byte AS number BGP speaker that contains AS path segments made up of more than one thousand autonomous systems, the device may crash with memory corruption, and the error "%Software-forced reload" will be displayed.

The following three conditions are required for successful exploitation of this vulnerability:

- Affected Cisco IOS Software device is a 4-byte AS number BGP speaker
- BGP peering neighbor is a 2-byte AS number BGP speaker
- BGP peering neighbor is capable of sending a BGP update with a series of greater than one thousand AS numbers

Note: Note: Cisco IOS, Cisco IOS XE, Cisco NX-OS and Cisco IOS XR Software, as a 2 byte AS number BGP speaker send BGP updates with a maximum of 255 AS numbers.

This vulnerability is documented in Cisco Bug ID [CSCsy86021](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-1168.

The second vulnerability could cause an affected device to reload when the affected device processes a malformed BGP update that has been crafted to trigger the issue. The following three conditions are required for successful exploitation of this vulnerability:

- Affected Cisco IOS Software device is a 4-byte AS number BGP speaker
- BGP peering neighbor is a 2-byte AS number BGP speaker
- BGP peering neighbor is capable of sending a non-RFC compliant crafted BGP update message

This vulnerability is documented in Cisco Bug ID [CSCta33973](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-2049.

Further information regarding Cisco support for 4-byte AS number is available in "Cisco IOS BGP 4-Byte ASN Support" at the following link:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6554/ps6599/data_sheet_C78-521821.html

[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>.

CSCsy86021: Cisco IOS Software BGP Long AS path Vulnerability					
Calculate the environmental score of CSCsy86021					
CVSS Base Score - 7.1					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	None	Complete
CVSS Temporal Score - 6.7					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCta33973: Cisco IOS Software Crafted BGP Update Message Vulnerability					
Calculate the environmental score of CSCta33973					
CVSS Base Score - 5.4					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	High	None	None	None	Complete
CVSS Temporal Score - 4.5					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

[Top of the section](#) [Close Section](#)

☐ Impact

Successful exploitation of the vulnerabilities described in this document may result in a reload of the device. The issue could result in repeated exploitation to cause an extended DoS condition.

[Top of the section](#) [Close Section](#)

☐ Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> 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) or your contracted maintenance provider for assistance.

Each row of the Cisco IOS software table (below) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. 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. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	Recommended Release
12.0	Not Vulnerable	
12.0DA	Not Vulnerable	
12.0DB	Not Vulnerable	
12.0DC	Not Vulnerable	
12.0S	Releases up to and including 12.0(32)S11 are not vulnerable; first fixed in 12.0(32)S14; Available on 25-Sep-2009; Releases up to and including 12.0(33)S2 are not vulnerable; first fixed in 12.0(33)S5	12.0(32)S14; Available on 25-Sep-2009
12.0SC	Not Vulnerable	
12.0SL	Not Vulnerable	
12.0SP	Not Vulnerable	
12.0ST	Not Vulnerable	
12.0SX	Not Vulnerable	
12.0SY	Releases up to and including 12.0(32)SY7 are not vulnerable; first fixed in 12.0(32)SY8b and 12.0(32)SY9a.	12.0(32)SY10; Available on 25-Sep-2009
12.0SZ	Not Vulnerable	
12.0T	Not Vulnerable	

12.0W	Not Vulnerable	
12.0WC	Not Vulnerable	
12.0WT	Not Vulnerable	
12.0WX	Not Vulnerable	
12.0XA	Not Vulnerable	
12.0XB	Not Vulnerable	
12.0XC	Not Vulnerable	
12.0XD	Not Vulnerable	
12.0XE	Not Vulnerable	
12.0XF	Not Vulnerable	
12.0XG	Not Vulnerable	
12.0XH	Not Vulnerable	
12.0XI	Not Vulnerable	
12.0XJ	Not Vulnerable	
12.0XK	Not Vulnerable	
12.0XL	Not Vulnerable	
12.0XM	Not Vulnerable	
12.0XN	Not Vulnerable	
12.0XQ	Not Vulnerable	
12.0XR	Not Vulnerable	
12.0XS	Not Vulnerable	
12.0XT	Not Vulnerable	
12.0XV	Not Vulnerable	
12.0XW	Not Vulnerable	
Affected 12.1-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.1 based releases		
Affected 12.2-Based Releases	First Fixed Release	Recommended Release
12.2	Not Vulnerable	
12.2B	Not Vulnerable	
12.2BC	Not Vulnerable	
12.2BW	Not Vulnerable	

12.2BX	Not Vulnerable	
12.2BY	Not Vulnerable	
12.2BZ	Not Vulnerable	
12.2CX	Not Vulnerable	
12.2CY	Not Vulnerable	
12.2CZ	Not Vulnerable	
12.2DA	Not Vulnerable	
12.2DD	Not Vulnerable	
12.2DX	Not Vulnerable	
12.2EW	Not Vulnerable	
12.2EWA	Not Vulnerable	
12.2EX	Not Vulnerable	
12.2EY	Not Vulnerable	
12.2EZ	Not Vulnerable	
12.2FX	Not Vulnerable	
12.2FY	Not Vulnerable	
12.2FZ	Not Vulnerable	
12.2IRA	Not Vulnerable	
12.2IRB	Not Vulnerable	
12.2IRC	Not Vulnerable	
12.2IXA	Not Vulnerable	
12.2IXB	Not Vulnerable	
12.2IXC	Not Vulnerable	
12.2IXD	Not Vulnerable	
12.2IXE	Not Vulnerable	
12.2IXF	Not Vulnerable	
12.2IXG	Not Vulnerable	
12.2IXH	Not Vulnerable	
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	Not Vulnerable	
12.2S	Not Vulnerable	
12.2SB	Not Vulnerable	

12.2SBC	Not Vulnerable	
12.2SCA	Not Vulnerable	
12.2SCB	Not Vulnerable	
12.2SE	Not Vulnerable	
12.2SEA	Not Vulnerable	
12.2SEB	Not Vulnerable	
12.2SEC	Not Vulnerable	
12.2SED	Not Vulnerable	
12.2SEE	Not Vulnerable	
12.2SEF	Not Vulnerable	
12.2SEG	Not Vulnerable	
12.2SG	Not Vulnerable	
12.2SGA	Not Vulnerable	
12.2SL	Not Vulnerable	
12.2SM	Not Vulnerable	
12.2SO	Not Vulnerable	
12.2SQ	Not Vulnerable	
12.2SRA	Not Vulnerable	
12.2SRB	Not Vulnerable	
12.2SRC	Not Vulnerable	
12.2SRD	Not Vulnerable	
12.2STE	Not Vulnerable	
12.2SU	Not Vulnerable	
12.2SV	Not Vulnerable	
12.2SVA	Not Vulnerable	
12.2SVC	Not Vulnerable	
12.2SVD	Not Vulnerable	
12.2SVE	Not Vulnerable	
12.2SW	Not Vulnerable	
12.2SX	Not Vulnerable	
12.2SXA	Not Vulnerable	
12.2SXB	Not Vulnerable	
12.2SXD	Not Vulnerable	
12.2SXE	Not Vulnerable	

12.2SXF	Not Vulnerable	
12.2SXH	Not Vulnerable	
12.2SXI	Releases up to and including 12.2(33)SXI are not vulnerable; First fixed in 12.2(33)SXI2a.	
12.2SY	Not Vulnerable	
12.2SZ	Not Vulnerable	
12.2T	Not Vulnerable	
12.2TPC	Not Vulnerable	
12.2XA	Not Vulnerable	
12.2XB	Not Vulnerable	
12.2XC	Not Vulnerable	
12.2XD	Not Vulnerable	
12.2XE	Not Vulnerable	
12.2XF	Not Vulnerable	
12.2XG	Not Vulnerable	
12.2XH	Not Vulnerable	
12.2XI	Not Vulnerable	
12.2XJ	Not Vulnerable	
12.2XK	Not Vulnerable	
12.2XL	Not Vulnerable	
12.2XM	Not Vulnerable	
12.2XN	Not Vulnerable	
12.2XNA	Not Vulnerable	
12.2XNB	Not Vulnerable	
12.2XNC	12.2(33)XNC2	
12.2XND	12.2(33)XND1; available 25th August 2009	
12.2XO	Not Vulnerable	
12.2XQ	Not Vulnerable	
12.2XR	Not Vulnerable	
12.2XS	Not Vulnerable	
12.2XT	Not Vulnerable	

12.2XU	Not Vulnerable	
12.2XV	Not Vulnerable	
12.2XW	Not Vulnerable	
12.2YA	Not Vulnerable	
12.2YB	Not Vulnerable	
12.2YC	Not Vulnerable	
12.2YD	Not Vulnerable	
12.2YE	Not Vulnerable	
12.2YF	Not Vulnerable	
12.2YG	Not Vulnerable	
12.2YH	Not Vulnerable	
12.2YJ	Not Vulnerable	
12.2YK	Not Vulnerable	
12.2YL	Not Vulnerable	
12.2YM	Not Vulnerable	
12.2YN	Not Vulnerable	
12.2YO	Not Vulnerable	
12.2YP	Not Vulnerable	
12.2YQ	Not Vulnerable	
12.2YR	Not Vulnerable	
12.2YS	Not Vulnerable	
12.2YT	Not Vulnerable	
12.2YU	Not Vulnerable	
12.2YV	Not Vulnerable	
12.2YW	Not Vulnerable	
12.2YX	Not Vulnerable	
12.2YY	Not Vulnerable	
12.2YZ	Not Vulnerable	
12.2ZA	Not Vulnerable	
12.2ZB	Not Vulnerable	
12.2ZC	Not Vulnerable	
12.2ZD	Not Vulnerable	
12.2ZE	Not Vulnerable	
12.2ZF	Not Vulnerable	

12.2ZG	Not Vulnerable	
12.2ZH	Not Vulnerable	
12.2ZJ	Not Vulnerable	
12.2ZL	Not Vulnerable	
12.2ZM	Not Vulnerable	
12.2ZP	Not Vulnerable	
12.2ZU	Not Vulnerable	
12.2ZX	Not Vulnerable	
12.2ZY	Not Vulnerable	
12.2ZYA	Not Vulnerable	
Affected 12.3-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.3 based releases		
Affected 12.4-Based Releases	First Fixed Release	Recommended Release
12.4	Not Vulnerable	
12.4JA	Not Vulnerable	
12.4JDA	Not Vulnerable	
12.4JDC	Not Vulnerable	
12.4JDD	Not Vulnerable	
12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MDA	Not Vulnerable	
12.4MR	Not Vulnerable	
12.4SW	Not Vulnerable	
12.4T	Releases up to 12.4(24) T are not vulnerable; first fixed in 12.4(24) T2 Available on 23- Oct-2009	12.4(24)T2; Available on 23- Oct-2009

12.4XA	Not Vulnerable	
12.4XB	Not Vulnerable	
12.4XC	Not Vulnerable	
12.4XD	Not Vulnerable	
12.4XE	Not Vulnerable	
12.4XF	Not Vulnerable	
12.4XG	Not Vulnerable	
12.4XJ	Not Vulnerable	
12.4XK	Not Vulnerable	
12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
12.4XP	Not Vulnerable	
12.4XQ	Not Vulnerable	
12.4XR	Not Vulnerable	
12.4XT	Not Vulnerable	
12.4XV	Not Vulnerable	
12.4XW	Not Vulnerable	
12.4XY	Not Vulnerable	
12.4XZ	Not Vulnerable	
12.4YA	Not Vulnerable	
12.4YB	Not Vulnerable	
12.4YD	Not Vulnerable	

Cisco IOS XE Release Table

Major Release	Availability of Repaired Releases
Affected 2.1 Based Releases	There are no affected 2.1 based releases
Affected 2.2 Based Releases	There are no affected 2.2 based releases
Affected 2.3 Based Releases	Releases up to and including 2.3.1t are vulnerable; First fixed in 2.3.2
Affected 2.4 Based Releases	Releases up to and including 2.4.0 are vulnerable; First fixed in 2.4.1, available 25th August 2009

☐ Workarounds

For the first vulnerability, there are no workarounds on the affected device. Neighbors could be configured to discard routes that have more than one thousand AS numbers in the AS-path segments. This configuration will help prevent the further propagation of BGP updates with the AS path segments made up of greater than one thousand AS numbers.

Note: Configuring "**bgp maxas-limit [value]**" on the affected device does **not** mitigate this vulnerability.

For the second vulnerability, configuring "**bgp maxas-limit [value]**" on the affected device **does** mitigate this vulnerability. Cisco recommends using a conservative value of 100 to mitigate this vulnerability.

Consult the document "Protecting Border Gateway Protocol for the Enterprise" at the following link for additional best practices on protecting BGP infrastructures:

http://www.cisco.com/web/about/security/intelligence/protecting_bgp.html

☐ Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. 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/en/US/docs/general/warranty/English/EU1KEN_.html, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including 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 malicious exploitation of either of these vulnerabilities, although we are aware of some customers who have seen the first vulnerability triggered within their infrastructures. Further investigation of those incidents seems to indicate that the vulnerability has been accidentally triggered.

These vulnerabilities were discovered via internal product testing.

[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 is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20090729-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-bulletins@lists.first.org
- 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.

[Top of the section](#) [Close Section](#)

☐ **Revision History**

Revision 1.2	2009-Aug-3	Modifications to insert 2 byte and 4 byte clarification at customer's request.
Revision 1.1	2009-July-30	Updated software table information for 12.0S, 12.0SY, and 12.4T
Revision 1.0	2009-July-29 1600	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 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>.

[Top of the section](#) [Close Section](#)

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)

Send

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

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)