

# Cisco Security Advisory: Cisco IOS XR Software Border Gateway Protocol Vulnerabilities

Advisory ID: cisco-sa-20090818-bgp

<http://www.cisco.com/warp/public/707/cisco-sa-20090818-bgp.shtml>

## Revision 2.6

Last Updated 2009 August 27 1500 UTC (GMT)

For Public Release 2009 August 18 1500 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

Cisco IOS XR Software contains multiple vulnerabilities in the Border Gateway Protocol (BGP) feature. These vulnerabilities include:

- Cisco IOS XR Software will reset a BGP peering session when receiving a specific invalid BGP

update.

The vulnerability manifests when a BGP peer announces a prefix with a specific invalid attribute. On receipt of this prefix, the Cisco IOS XR device will restart the peering session by sending a notification. The peering session will flap until the sender stops sending the invalid/corrupt update. This vulnerability was disclosed in revision 1.0 of this advisory.

- Cisco IOS XR BGP process will crash when sending a long length BGP update message  
When Cisco IOS XR sends a long length BGP update message, the BGP process may crash. The number of AS numbers required to exceed the total/maximum length of update message and cause the crash are well above normal limits seen within production environments.
- Cisco IOS XR BGP process will crash when constructing a BGP update with a large number of AS prepends  
If the Cisco IOS XR BGP process is configured to prepend a very large number of Autonomous System (AS) Numbers to the AS path, the BGP process will crash. The number of AS numbers required to be prepended and cause the crash are well above normal limits seen within production environments.

All three vulnerabilities are different vulnerabilities from what was disclosed in the Cisco Security Advisory "Cisco IOS Software Border Gateway Protocol 4-Byte Autonomous System Number Vulnerabilities" on the 2009 July 29 1600 UTC at the following link:

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

Cisco has released a free software maintenance upgrade (SMU) that addresses these vulnerabilities.

Workarounds that mitigates these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090818-bgp.shtml>

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

## ☐ Affected Products

The "Cisco IOS XR Software will reset a BGP peering session when receiving a specific invalid BGP update" vulnerability affects all Cisco IOS XR Software devices after and including software release 3.4.0 configured with BGP routing.

The other two vulnerabilities affect all Cisco IOS XR Software devices configured with BGP routing.

## ☐ Vulnerable Products

To determine the Cisco IOS XR 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 XR Software by displaying text similar to "Cisco IOS XR Software". The software version is displayed after the text "Cisco IOS XR Software".

The following example identifies a Cisco CRS-1 that is running Cisco IOS XR Software Release

### 3.6.2:

```
RP/0/RP0/CPU0:CRS#show version
Tue Aug 18 14:25:17.407 AEST

Cisco IOS XR Software, Version 3.6.2[00]
Copyright (c) 2008 by Cisco Systems, Inc.

ROM: System Bootstrap, Version 1.49(20080319:195807) [CRS-1 ROMMON],

CRS uptime is 4 weeks, 4 days, 1 minute
System image file is "disk0:hfr-os-mbi-3.6.2/mbihfr-rp.vm"

cisco CRS-8/S (7457) processor with 4194304K bytes of memory.
7457 processor at 1197Mhz, Revision 1.2

17 Packet over SONET/SDH network interface(s)
1 DWDM controller(s)
17 SONET/SDH Port controller(s)
8 TenGigabitEthernet/IEEE 802.3 interface(s)
2 Ethernet/IEEE 802.3 interface(s)
1019k bytes of non-volatile configuration memory.
38079M bytes of hard disk.
981440k bytes of ATA PCMCIA card at disk 0 (Sector size 512 bytes).

Configuration register on node 0/0/CPU0 is 0x102
Boot device on node 0/0/CPU0 is mem:
```

*!--- output truncated*

The following example identifies a Cisco 12404 router that is running Cisco IOS XR Software Release 3.7.1:

```
RP/0/0/CPU0:GSR#show version

Cisco IOS XR Software, Version 3.7.1[00]
Copyright (c) 2008 by Cisco Systems, Inc.

ROM: System Bootstrap, Version 12.0(20051020:160303) SOFTWARE
Copyright (c) 1994-2005 by cisco Systems, Inc.

GSR uptime is 3 weeks, 6 days, 3 hours, 20 minutes
System image file is "disk0:c12k-os-mbi-3.7.1/mbiprp-rp.vm"

cisco 12404/PRP (7457) processor with 2097152K bytes of memory.
7457 processor at 1266Mhz, Revision 1.2

1 Cisco 12000 Series Performance Route Processor
1 Cisco 12000 Series - Multi-Service Blade Controller
1 1 Port ISE Packet Over SONET OC-48c/STM-16 Controller (1 POS)
1 Cisco 12000 Series SPA Interface Processor-601/501/401
3 Ethernet/IEEE 802.3 interface(s)
1 SONET/SDH Port controller(s)
1 Packet over SONET/SDH network interface(s)
4 PLIM QoS controller(s)
8 FastEthernet/IEEE 802.3 interface(s)
1016k bytes of non-volatile configuration memory.
```

```
1000496k bytes of disk0: (Sector size 512 bytes).
65536k bytes of Flash internal SIMM (Sector size 256k).
```

```
Configuration register on node 0/0/CPU0 is 0x2102
Boot device on node 0/0/CPU0 is disk0:
```

*!--- output truncated*

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

<http://www.cisco.com/warp/public/620/1.html#t6>.

Additional information about Cisco IOS XR Software time-based release model is available in the "White Paper: Guidelines for Cisco IOS XR Software" at the following link:

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8803/ps5845/product\\_bulletin\\_c25-478699.html](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8803/ps5845/product_bulletin_c25-478699.html).

BGP is configured in Cisco IOS XR Software with the configuration command **router bgp [AS Number]** or **router bgp [X.Y]**. The device is vulnerable if it is running an affected Cisco IOS XR Software version and has BGP configured.

The following example shows a Cisco IOS XR Software device configured with BGP:

```
RP/0/0/CPU0:GSR#show running-config | begin router bgp
Building configuration...
router bgp 65535
  bgp router-id 192.168.0.1
  address-family ipv4 unicast
    network 192.168.1.1/32
  !
  address-family vpnv4 unicast
  !
  neighbor 192.168.2.1
    remote-as 65534
    update-source Loopback0
  address-family ipv4 unicast
  !
```

*!--- output truncated*

## ☐ Products Confirmed Not Vulnerable

The following Cisco products are confirmed not vulnerable:

- Cisco IOS Software
- Cisco IOS XR Software not configured for BGP routing

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

## ▣ Details

These vulnerabilities affect Cisco IOS XR devices running affected software versions and configured with the BGP routing feature. Details per vulnerability are outlined below:

- Cisco IOS XR Software will reset a BGP peering session when receiving a specific invalid BGP update.

On August 17th, 2009, a widely-distributed Border Gateway Protocol (BGP) route update contained a BGP Update message with a specific invalid attribute. When the invalid BGP Update message was processed by Cisco IOS XR Software, it began resetting BGP peering sessions over which the update was received.

When a affected device receives the invalid/corrupt update, Cisco IOS XR Software will create a log message like the following example:

```
RP/0/RP0/CPU0:Aug 17 13:47:05.896 GMT: bgp[122]: %ROUTING-BGP-5-ADJCHAN
```

The peering session will flap until the sender stops sending the invalid/corrupt BGP update message.

This vulnerability is documented in Cisco Bug ID [CSCtb42995](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-2055.

- Cisco IOS XR BGP process will crash when sending a long length BGP update message  
The BGP process on an affected Cisco IOS XR device may reload when sending a long length BGP update. The number of AS numbers required to exceed the total/maximum length of update message and cause the crash are well above normal limits seen within production environments.

When an affected device BGP process crashes because of this long length BGP update message, Cisco IOS XR Software may create a log message like the following example:

```
bgp[122]: %ROUTING-BGP-3-INTERNAL_ERROR : [10] : Internal error (Write
```

The above error message is not always displayed and the BGP process may crash before IOS XR has the chance to generate the error message.

This vulnerability is documented in Cisco Bug ID [CSCtb05382](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-1154.

- Cisco IOS XR BGP process will crash when constructing a BGP update with a large number of AS prepends  
If the Cisco IOS XR BGP process is configured to prepend a very large number of AS Numbers to the AS path, the BGP process will crash. The number of AS numbers required to be prepended to cause the crash are well above normal limits seen within production environments.

An example of AS path prepending in Cisco IOS XR Software is shown below:

```
route-policy prepend-example
  prepend as-path 65534 3
  prepend as-path 65531 2
```

```

end-policy

router bgp 65534
  neighbor 192.168.0.1
  remote-as 65531
  address-family ipv4 unicast
    route-policy prepend-example out

```

When an affected device BGP process crashes because of this large AS path prepend, no log message will be generated, prior to the crash.

This vulnerability is documented in Cisco Bug ID [CSCtb12726](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-2056.

The above three vulnerabilities have been fixed in a single SMU and released under an umbrella Cisco Bug ID [CSCtb18562](#) ([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> .

CSCtb42995/CSCtb05382: Cisco IOS XR Software Border Gateway Protocol Vulnerabilities					
Calculate the environmental score of <a href="#">CSCtb42995/CSCtb05382</a>					
CVSS Base Score - <b>4.3</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	None	Partial

CVSS Temporal Score - <b>3.6</b>		
Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

<b>CSCctb12726: Cisco IOS XR BGP process will crash when constructing a BGP update with a large number of AS prepends</b>					
Calculate the environmental score of <a href="#">CSCctb12726</a>					
CVSS Base Score - <b>3.3</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Multiple	None	None	Partial
CVSS Temporal Score - <b>2.7</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

## ☐ Impact

Successful exploitation of these vulnerabilities may result in the continuous resetting of BGP peering sessions, or the continuous resetting of the BGP process itself. This may lead to routing inconsistencies and a denial of service for those affected networks.

[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.

**Note:** Currently the SMUs are being posted to Cisco.com. This section will be updated accordingly once the SMUs are available for download.

Cisco IOS XR Version	SMU ID	SMU Name
	Vulnerable to BGP	

3.2.X	process crash vulnerabilities; Migrate to 3.4.1 or later.	
3.3.X	Vulnerable to BGP process crash vulnerabilities; Migrate to 3.4.1 or later.	
3.4.0	Vulnerable; Migrate to 3.4.1 or later.	
3.4.1	AA03400 AA03414	hfr-rout-3.4.1.CSCtb18562 c12k-rout-3.4.1.CSCtb18562
3.4.2	AA03399 AA03413	hfr-rout-3.4.2.CSCtb18562 c12k-rout-3.4.2.CSCtb18562
3.4.3	AA03398 AA03412	hfr-rout-3.4.3.CSCtb18562 c12k-rout-3.4.3.CSCtb18562
3.5.2	AA03397 AA03411	hfr-rout-3.5.2.CSCtb18562 c12k-rout-3.5.2.CSCtb18562
3.5.3	AA03410 AA03396	c12k-rout-3.5.3.CSCtb18562 hfr-rout-3.5.3.CSCtb18562
3.5.4	AA03409 AA03395	c12k-rout-3.5.4.CSCtb18562 hfr-rout-3.5.4.CSCtb18562
3.6.0	AA03394 AA03408	hfr-rout-3.6.0.CSCtb18562 c12k-rout-3.6.0.CSCtb18562
		c12k-rout-

3.6.1	AA03407	3.6.1.CSCtb18562
	AA03393	hfr-rout- 3.6.1.CSCtb18562
3.6.2	AA03406	c12k-rout- 3.6.2.CSCtb18562
	AA03392	hfr-rout- 3.6.2.CSCtb18562
3.6.3	AA03405	c12k-rout- 3.6.3.CSCtb18562
	AA03391	hfr-rout- 3.6.3.CSCtb18562
3.7.0	AA03390	hfr-rout- 3.7.0.CSCtb18562
	AA03404	c12k-rout- 3.7.0.CSCtb18562
3.7.1	AA03389	hfr-rout- 3.7.1.CSCtb18562
	AA03403	c12k-rout- 3.7.1.CSCtb18562
3.7.2	AA03386	asr9k-rout- 3.7.2.CSCtb18562
3.7.3	AA03385	asr9k-rout- 3.7.3.CSCtb18562
3.8.0	AA03388	hfr-rout- 3.8.0.CSCtb18562
	AA03402	c12k-rout- 3.8.0.CSCtb18562
3.8.1	AA03401	hfr-rout- 3.8.1.CSCtb18562
	AA03387	c12k-rout- 3.8.1.CSCtb18562

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

## ☐ Workarounds

Each individual vulnerability has a different workaround. Following are the mitigations and workarounds recommended for these vulnerabilities, prior to applying a SMU or software upgrade.

The workarounds should be applied to both eBGP and iBGP peers.

- Cisco IOS XR Software will reset a BGP peering session when receiving a specific invalid BGP update.

There are no workarounds on the affected device itself. Co-ordination is required with the peering neighbor support staff to filter the invalid update on their outbound path. The following procedure explains how to help mitigate this vulnerability:

Using the peer IP address in the log message that was generated when the Cisco IOS XR Software device received the invalid update; capture the notification message hex dump from the CLI command **show bgp neighbor** and contact the Cisco TAC, who can assist with a decode. Details on how to contact Cisco TAC are contained within the "Obtaining Fixed Software" section of this advisory.

For illustrative purposes, the following example shows a log message generated by an affected device when it receives an invalid/corrupt update message:

```
RP/0/RP0/CPU0:Aug 17 13:47:05.896 GMT: bgp[122]: %ROUTING-BGP-5-ADJCHAN
```

These details can be captured and provided to Cisco TAC to decode the update message. **show bgp neighbors [ip address of neighbor from above log message]:**

```
RP/0/RP0/CPU0:CRS#show bgp neighbors 192.168.0.1
```

```
<capture output and provide to Cisco TAC>
```

Working with Cisco TAC, the decode of the above will display the AS path in a manner illustrated below.

```
ATTRIBUTE NAME: AS_PATH
```

```
AS_PATH: Type 2 is AS_SEQUENCE
```

```
AS_PATH: Segment Length is 4 (0x04) segments long
```

```
AS_PATH: 65533 65532 65531 65531
```

Working cooperatively with your peering partner, request that they filter outbound prefix advertisements from the identified source AS (in this example 65531) for your peering session. The filters configuration methods will vary depending on the routing device operating system used. For Cisco IOS XR Software the filters will be applied using Routing Policy Language (RPL) policies or with Cisco IOS Software via applying route-maps that deny advertisements matching that AS in their AS-PATH. Once these policies are applied, the peering session will be re-established.

For further information on Cisco IOS XR RPL consult the document "Implementing Routing Policy on Cisco IOS XR Software" at the following link:

[http://www.cisco.com/en/US/docs/ios\\_xr\\_sw/iosxr\\_r3.0/routing/configuration/guide/rc3rpl.htm](http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.0/routing/configuration/guide/rc3rpl.htm)

For further information on Cisco IOS route maps with BGP, consult the document "Cisco IOS BGP Configuration Guide, Release 12.4T" at the following link:

[http://www.cisco.com/en/US/docs/ios/12\\_2sr/12\\_2srb/feature/guide/tbgp\\_c.html](http://www.cisco.com/en/US/docs/ios/12_2sr/12_2srb/feature/guide/tbgp_c.html).

- Cisco IOS XR BGP process will crash when sending a long length BGP update message

While the long length BGP update message can be caused by any number of attributes, then most common would be the AS Path. Limiting the number of AS numbers in the AS Path Attribute should mitigate this vulnerability. The following shows an example of filtering on AS paths within Cisco IOS XR Software:

```
route-policy maxas-limit
# Check number of AS Numbers in AS Path attribute.
# If greater than 100 drop the update.
# If less than 100 pass the update.
  if as-path length ge 100 then
    drop
  else
    pass
  endif
end-policy

router bgp 65533
neighbor 192.168.0.1
remote-as 65534
address-family ipv4 unicast
  policy maxas-limit in
  policy maxas-limit out
```

For further information on Cisco IOS XR RPL consult the document "Implementing Routing Policy on Cisco IOS XR Software" at the following link:  
[http://www.cisco.com/en/US/docs/ios\\_xr\\_sw/iosxr\\_r3.0/routing/configuration/guide/rc3rpl.htm](http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.0/routing/configuration/guide/rc3rpl.htm)

- Cisco IOS XR BGP process will crash when constructing a BGP update with a large number of AS prepends  
There is no workaround for this vulnerability, other than reducing the number of AS path prepends configured within Cisco IOS XR.

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

## ☐ Obtaining Fixed Software

Cisco will be releasing 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](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](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto: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](mailto: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](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**

On August 17, 2009 around 16:30-17:00 UTC several ISP's began experiencing connectivity issues as BGP sessions were being repeatedly reset, which corresponds to the vulnerability "Cisco IOS XR will reset a BGP peering session when receiving a specific invalid BGP update" disclosed in this advisory. Cisco TAC was engaged with a number of customers all seeing similar issues. Stability came a few hours afterward as workarounds were applied. At this time, it is not believed that the connectivity issues were the result of malicious activity.

The other two BGP process crash vulnerabilities were discovered by Cisco during internal negative 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-20090818-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](mailto:cust-security-announce@cisco.com)
- [first-bulletins@lists.first.org](mailto:first-bulletins@lists.first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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 2.6	2009- August-27	Minor revision to software table
Revision 2.5	2009- August-24	Added final SMUs to the Software Table.
Revision 2.4	2009- August-23	Added newly available SMUs to the Software Table.

Revision 2.3	2009-August-22	Added newly available SMUs to the Software Table.
Revision 2.2	2009-August-21	Added newly available SMUs to the Software Table.
Revision 2.1	2009-August-20	Added currently available SMUs to the Software Table and separated CVSS tables.
Revision 2.0	2009-August-20	Major update to include all bugs in Umbrella fix.
Revision 1.0	2009-August-18	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](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

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

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

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