

Cisco Security Advisory: Vulnerability in Cisco IOS with OSPF, MPLS VPN, and Supervisor 32, Supervisor 720, or Route Switch Processor 720

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-03/msg00346.html>

- *From:* Cisco Systems Product Security Incident Response Team <psirt@xxxxxxxx>
 - *Date:* Wed, 26 Mar 2008 17:00:00 +0100
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Cisco Security Advisory: Vulnerability in Cisco IOS with OSPF, MPLS VPN, and Supervisor 32, Supervisor 720, or Route Switch Processor 720

Advisory ID: cisco-sa-20080326-queue

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-queue.shtml>

Revision 1.0

For Public Release 2008 March 26 1600 UTC (GMT)

Summary

=====

Certain Cisco Catalyst 6500 Series and Cisco 7600 Router devices that run branches of Cisco IOS based on 12.2 can be vulnerable to a denial of service vulnerability that can prevent any traffic from entering an affected interface. For a device to be vulnerable, it must be configured for Open Shortest Path First (OSPF) Sham-Link and Multi Protocol Label Switching (MPLS) Virtual Private Networking (VPN). This vulnerability only affects Cisco Catalyst 6500 Series or Catalyst 7600 Series devices with the Supervisor Engine 32 (Sup32), Supervisor Engine 720 (Sup720) or Route Switch Processor 720 (RSP720) modules. The Supervisor 32, Supervisor 720, Supervisor 720-3B, Supervisor 720-3BXL, Route Switch Processor 720, Route Switch Processor 720-3C, and Route Switch Processor 720-3CXL are all potentially vulnerable.

The OSPF and MPLS VPNs are not enabled by default.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-queue.shtml>

Cisco Security Advisory: Vulnerability in Cisco IOS with OSPF, MPLS VPN, and Supervisor 32, Supervisor 720, or Route Switch Processor 720

Note: The March 26, 2008 publication includes five Security Advisories. The Advisories all affect Cisco IOS. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities in all five Advisories. Please reference the following software table to find a release which fixes all published Security Advisories as of March 26th, 2008.

* March 26th bundled IOS Advisory Table

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-bundle.shtml>

Individual publication links are listed below:

* Cisco IOS Virtual Private Dial-up Network Denial of Service Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-pptp.shtml>

* Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml>

* Cisco IOS User Datagram Protocol Delivery Issue For IPv4/IPv6 Dual-stack Routers

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml>

* Vulnerability in Cisco IOS with OSPF, MPLS VPN, and Supervisor 32, Supervisor 720, or Route Switch Processor 720

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-queue.shtml>

* Cisco IOS Multicast Virtual Private Network (MVPN) Data Leak

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml>

Affected Products

=====

Vulnerable Products

+-----

All Cisco products based on the Supervisor Engine 32 (Sup32), Supervisor Engine 720 (Sup720) or Route Switch Processor 720 (RSP720) are potentially vulnerable. Cisco Sup720 and RSP720 products have support for daughter cards that enhance their functionality. These daughter cards attach directly to the Sup720 or RSP720 and have names like PFC-3B, PFC-3BXL, PFC-3C, and PFC-3CXL. The product number of the Sup720 or RSP720 can change to reflect the daughter card that is installed, such as RSP720-3CXL.

Because the vulnerability affects the Sup720 and RSP720, all versions of the Sup720 or RSP720 are vulnerable, regardless of the daughter card that is installed.

- * Cisco Catalyst 6500 Series devices with the Sup32, Sup720, Sup720-3B, or Sup720-3BXL
- * Cisco 7600 Series devices with the Sup32, Sup720, Sup720-3B, or Sup720-3BXL
- * Cisco 7600 Series devices with the RSP720, RSP720-3C, or RSP720-3CXL
- * Cisco ME 6524 Ethernet Switch

Products Confirmed Not Vulnerable

+-----

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

Cisco Bug ID CSCsf12082 was integrated into additional IOS releases that do not run on the vulnerable hardware, but only the platforms mentioned in the Vulnerable Products section above are affected by this vulnerability.

Details

=====

Vulnerable Cisco devices, when configured for Multi Protocol Label Switching (MPLS) Virtual Private Networking (VPN) and Open Shortest Path First (OSPF) sham-link, can suffer from a blocked queue, memory leak and/or restart of the device

This vulnerability is documented in Cisco bug ID CSCsf12082, and has been assigned CVE ID CVE-2008-0057.

The following combination of hardware and software configuration must be present for the device to be vulnerable:

- * Cisco Catalyst Sup32, Sup720, or RSP720 is present
- * MPLS VPN is configured
- * OSPF sham-link is configured

In order to determine whether you are running this feature, use the show running-config command and search for the address-family vpv4 and area sham-link router configuration commands. The following command displays all configuration lines that meet the following criteria:

- * Begins with the word "router," OR
- * Includes "address-family vpv4," OR
- * Includes "sham-link"

```
Router# show run | include ^router |address-family vpv4|sham-link
router bgp 1
address-family vpv4
```

```
router ospf 1 vrf VRFNAME
area 0 sham-link 192.168.1.1 192.168.100.1
Router#
```

For customers that run versions of IOS that support the section modifier, an additional option is available to view the relevant sections of the running configuration:

```
Router# show run | section ^router
router bgp 1
[snip]
address-family vpnv4
router ospf 1 vrf VRFNAME
area 0 sham-link 192.168.1.1 192.168.100.1
[snip]
```

If certain packets are received by a device that meets the above requirements, the input queue of the interface that receives these packets can become blocked, which can prohibit additional traffic from entering the interface and cause a denial of service condition. In addition to a potential blocked interface queue, the device can also suffer a memory leak or restart. In the event of a memory leak, the device is unable to forward traffic once available memory is depleted.

For more information on MPLS VPNs, please reference the following document:

http://www.cisco.com/en/US/docs/net_mgmt/vpn_solutions_center/1.1/user/guide/VPN_UG1.html

For more information on OSPF sham-links, please reference the following document:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ospfshmk.html

Identifying a Memory Leak

+-----

This vulnerability can manifest as a leak in the I/O memory pool. The following is an example of a system message that indicates an exhaustion of the I/O pool:

```
006029: Aug 10: %SYS-2-MALLOCFAIL: Memory allocation of 808 bytes failed from 0x41613238,
alignment 32
```

```
Pool: I/O Free: 176 Cause: Not enough free memory
```

```
Alternate Pool: None Free: 0 Cause: No Alternate pool
```

Note that in the above output, the affected memory pool is Pool: I/O, and the cause is Cause: Not enough free memory. This output indicates that the I/O memory pool has been exhausted.

Additionally, a user with enable-level access can check the device through the show buffers command to identify buffer allocation failures.

```
Router#show buffers
Buffer elements:
496 in free list (500 max allowed)
77298300 hits, 0 misses, 0 created
```

```
Public buffer pools:
Small buffers, 104 bytes (total 148654, permanent 1024, peak 148654 @ 1d12h):
0 in free list (128 min, 2048 max allowed)
24688031 hits, 4023203 misses, 0 trims, 147630 created
3243434 failures (3182828 no memory)
```

The above output shows that buffer allocation failed due to insufficient memory.

Identifying a Blocked Interface

+-----

A symptom of this type of blocked queue is the failure of control-plane protocols such as routing protocols (OSPF, Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), Intermediate System to Intermediate System (ISIS), etc.) and MPLS TDP/LDP to properly establish connections over an affected interface.

In order to identify a blocked input interface, issue the show interfaces command, and search for the Input Queue line. The size of the input queue can continue to increase. If the current size, which is 76 in the example below, is larger than the maximum size (75), the input queue is blocked.

It is possible that a device receives a high rate of traffic destined to the control plane, and the full queue is only a transient event. In order to verify if the interface is actually blocked, shut down the interface with the shutdown interface configuration command and examine the input queue. If the input queue does not display 0 packets, the interface is blocked.

```
Router#show interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
Hardware is AmdP2, address is 0050.500e.f1e0 (bia 0050.500e.f1e0)
Internet address is 172.16.1.9/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:41, output 00:00:07, output hang never
Last clearing of "show interface" counters 00:07:18
Input queue: 76/75/1091/0 (size/max/drops/flushes); Total output drops: 0
```

!---- The 76/75 shows that this is blocked

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>

CSCsf12082 – SUP720 facing small buffer leak and crashes

CVSS Base Score – 7.8

Access Vector: Network
Access Complexity: Low
Authentication: None

Confidentiality Impact: None
Integrity Impact: None
Availability Impact: Complete

CVSS Temporal Score – 6.1

Exploitability: Proof-of-Concept
Remediation Level: Official-Fix
Report Confidence: Confirmed

Impact
=====

Exploitation of this vulnerability may result in a blocked interface input queue, memory leak, and/or restart of the device. Repeated

exploitation of this vulnerability may result in an extended denial of service.

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	First Fixed Release	Recommended Release
12.0-Based	There are no affected 12.0 based releases		
12.1-Based	There are no affected 12.1 based releases		
12.2-Based			

12.2	Not	Vulnerable
12.2B	Not	Vulnerable
12.2BC	Not	Vulnerable
12.2BW	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
12.2EU	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
12.2IXA	Vulnerable;	contact TAC
12.2IXB	Vulnerable;	contact TAC
12.2IXC	Vulnerable;	contact TAC
12.2IXD	Vulnerable;	contact TAC
12.2IXE	Vulnerable; 12.2(18)	migrate to IXF; any release Available in 12.2IXF on 31-MAR-2008
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
12.2SE	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
12.2SRA	12.2(33) 12.2(33) SRA4 SRA7	
12.2SRB	Not	Vulnerable
12.2SRC	Not	Vulnerable

12.2SU	Not	Vulnerable
12.2SV	Not	Vulnerable
12.2SVA	Not	Vulnerable
12.2SVC	Not	Vulnerable
12.2SVD	Not	Vulnerable
12.2SW	Not	Vulnerable
12.2SX	Not	Vulnerable
12.2SXA	first fixed	SXF13
	in	12.2SXF
12.2SXB	first fixed	SXF13
	in	12.2SXF
12.2SXD	first fixed	SXF13
	in	12.2SXF
12.2SXE	first fixed	SXF13
	in	12.2SXF
12.2SXF	12.2(18)	12.2(18)
	SXF6	SXF13
12.2SXH	Not	Vulnerable
12.2SY	Not	Vulnerable
12.2SZ	Not	Vulnerable
12.2T	Not	

Vulnerable		
12.2TPC	Not	
Vulnerable		
12.2UZ	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		
12.2XO	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		
12.2ZP	Not	
Vulnerable		
Vulnerable;		
12.2ZU	migrate to 12.2(33)	
any release	SXH2	
in 12.2SXH		
12.2ZY	Not	
Vulnerable		
Affected	First Fixed	Recommended
12.3-Based	Release	Release
Releases		
There are no affected 12.3 based releases		
Affected	First Fixed	Recommended
12.4-Based	Release	Release
Releases		
There are no affected 12.4 based releases		

Workarounds

=====

Once a device interface queue has been exhausted, only a device restart can clear OSPF packets in the blocked queue.

Due to the manner in which these packets are processed, the queue block occurs prior to the OSPF MD5 check. The OSPF MD5 configuration does not protect a device from this vulnerability.

Increasing the Selective Packet Discard (SPD) Headroom

+-----

At the most basic level, the Selective Packet Discard (SPD) provides extended buffering for control plane traffic. Known as the SPD headroom, this additional queue depth is typically reserved for traffic with IP Precedence equal to 6 (such as BGP), the Connectionless Network Service (CLNS) based routing protocol Intermediate System-to-Intermediate System (IS-IS), OSPF, and Layer 2 keepalives.

Increasing the SPD headroom provides additional buffering for OSPF packets. In the event of a blocked queue, the SPD headroom can be increased to allow more control plane traffic buffer space.

More information on SPD can be found in the following white paper:

<http://www.cisco.com/web/about/security/intelligence/spd.html>

It is possible to expand the queue size to accommodate more packets, but packets can still accumulate until the expanded queue is exhausted. As a temporary workaround that allows traffic to continue to flow, the input hold queue can be increased. Any additional malformed packets still fill the queue, but increasing the input queue depth can extend the amount of time before the input queue fills and traffic ceases flowing. The following example demonstrates how to set the input queue size from the default of 75 to the maximum of 4096:

```
Router# configure terminal
Router(configure)# interface FastEthernet 0/0
Router(config-if)# hold-queue 4096 in
```

Removing OSPF Sham-Link Configuration

+-----

Because OSPF Sham-Link configuration is required for the vulnerability to be present, removing Sham-Link functionality eliminates exposure to this vulnerability. In order to remove the OSPF Sham-Link configuration from a device, the OSPF configuration

must be changed on each interface where Sham-Link is configured.

For configuration information on OSPF Sham-Link, please consult the following document:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ospfshmk.html

Cisco IOS Embedded Event Manager

+-----

Cisco IOS Embedded Event Manager (EEM) provides event detection and reaction capabilities on a Cisco IOS device. It is possible to detect blocked interface queues with an EEM policy. EEM can alert administrators of blocked interfaces with email, a syslog message, or a Simple Network Management Protocol (SNMP) trap.

A sample EEM policy that uses syslog to alert administrators of blocked interfaces is available at Cisco Beyond, an online community dedicated to EEM. A sample script is available at the following link:

<http://forums.cisco.com/eforum/servlet/EEM?page=eem&fn=script&scriptId=981>

More information about EEM is available from Cisco.com at the following link:

http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.html

Obtaining Fixed Software

=====

Cisco has released free software updates that address this vulnerability. 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/products/prod_warranties_item09186a008088e31f.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@xxxxxxxx or security-alert@xxxxxxxx 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@xxxxxxxxx

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/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

=====

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

This vulnerability was reported to Cisco by a customer.

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 is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-queue.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@xxxxxxxxxx
- * first-teams@xxxxxxxxxx
- * bugtraq@xxxxxxxxxxxxxxxxxxxxx
- * vulnwatch@xxxxxxxxxxxxxxxxxx
- * cisco@xxxxxxxxxxxxxxxxxxxxx
- * cisco-nsp@xxxxxxxxxxxxxxxxxxxxx
- * full-disclosure@xxxxxxxxxxxxxxxxxxxxx
- * comp.dcom.sys.cisco@xxxxxxxxxxxxxxxxxxxxx

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	Initial
1.0	2008-March-26 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>.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.8 (Darwin)

iEYEARECAAYFAkfb/IACgkQ86n/Gc8U/uDSVQCcD/eTXkZUyMzZERQXt+d9DhGD
dKgAnjQ+Gsmkh4/x115K8q2E9QKUJN1d
=xTuf

-----END PGP SIGNATURE-----