

# Cisco Security Advisory: Cisco IOS Software TCP Initial Sequence Number Randomization Improvements

Document ID: 13631

Advisory ID: cisco-sa-20010301-ios-tcp-isn-random

<http://www.cisco.com/warp/public/707/cisco-sa-20010301-ios-tcp-isn-random>

## Revision 1.3

Last Updated 2004 January 07 0830 UTC (GMT)

For Public Release 2001 March 01 0200 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: INTERIM
- Distribution
- Revision History
- Cisco Security Procedures

---

## Summary

Cisco IOS<sup>®</sup> Software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.

This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.

To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is described in DDTS record CSCds04747.

Workarounds are available that limit or deny successful exploitation of the vulnerability by filtering traffic containing forged IP source addresses at the perimeter of a network or directly on individual devices.

This notice will be posted at  
<http://www.cisco.com/warp/public/707/cisco-sa-20010301-ios-tcp-isn-random.shtml>.

## Affected Products

This section provides details on affected products.

### Vulnerable Products

The vulnerability is present in all Cisco routers and switches running affected releases of Cisco IOS Software.

To determine the software running on a Cisco product, log in to the device and issue the command "**show version**" to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS (tm)". On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the "**show version**" command or will give different output.

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

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

Cisco devices that may be running an affected IOS software release include, but are not limited to:

- 800, 1000, 1005, 1400, 1600, 1700, 2500, 2600, 3600, MC3810, 4000, 4500, 4700, 6200, 6400 NRP, 6400 NSP series Cisco routers.
- ubr900 and ubr920 universal broadband routers.
- Catalyst 2900 ATM, 2900XL, 2948g, 3500XL, 4232, 4840g, 5000 RSFC series switches.
- 5200, 5300, 5800 series access servers.
- Catalyst 6000 MSM, 6000 Hybrid Mode, 6000 Native Mode, 6000 Supervisor Module, Catalyst ATM Blade.
- RSM, 7000, 7010, 7100, 7200, ubr7200, 7500, 10000 ESR, and 12000 GSR series Cisco routers.
- DistributedDirector.
- Catalyst 8510CSR, 8510MSR, 8540CSR, 8540MSR series switches.

### Products Confirmed Not Vulnerable

Cisco products that do not run Cisco IOS software and are not affected by the vulnerabilities described in this notice include, but are not limited to:

- Cisco PIX firewall.
- Cisco 600 family of routers running CBOS.
- Host-based network management or access management products.
- Cisco IP Telephony and telephony management software (except those that are hosted on a vulnerable IOS platform).
- Voice gateways and convergence products (except those that are hosted on a vulnerable IOS platform).

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

## Details

To provide reliable delivery in the Internet, the Transmission Control Protocol (TCP) makes use of a sequence number in each packet to provide orderly reassembly of data after arrival, and to notify the sending host of the successful arrival of the data in each packet.

TCP sequence numbers are 32-bit integers in the circular range of 0 to 4,294,967,295. The host devices at both ends of a TCP connection exchange an Initial Sequence Number (ISN) selected at random from that range as part of the setup of a new TCP connection. After the session is established and data transfer begins, the sequence number is regularly augmented by the number of octets transferred, and transmitted to the other host. To prevent the receipt and reassembly of duplicate or late packets in a TCP stream, each host maintains a "window", a range of values close to the expected sequence number, in which the sequence number in an arriving packet must fall if it is to be accepted. Assuming a packet arrives with the correct source and destination IP addresses, source and destination port numbers, and a sequence number within the allowable window, the receiving host will accept the packet as genuine.

This method provides reasonably good protection against accidental receipt of unintended data. However, to guard against malicious use, it should not be possible for an attacker to infer a particular number in the sequence. If the initial sequence number is not chosen randomly or if it is incremented in a non-random manner between the initialization of subsequent TCP sessions, then it is possible, with varying degrees of success, to forge one half of a TCP connection with another host in order to gain access to that host, or hijack an existing connection between two hosts in order to compromise the contents of the TCP connection. To guard against such compromises, ISNs should be generated as randomly as possible.

This defect, documented as DDTS CSCds04747, has been corrected by providing an improved method for generating TCP Initial Sequence Numbers.

## Impact

Forged packets can be injected into a network from a location outside its boundary so that they are trusted as authentic by the receiving host, thus resulting in a failure of integrity. Such packets could be crafted to gain access or make some other modification to the receiving system in order to attain some goal, such as gaining unauthorized interactive access to a system or compromising stored data.

From a position within the network where it is possible to receive the return traffic (but not necessarily in a position that is directly in the traffic path), a greater range of violations is possible. For example, the contents of a message could be diverted, modified, and then returned to the traffic flow again, causing a failure of integrity and a possible failure of confidentiality.

**Note: Any compromise using this vulnerability is only possible for TCP sessions that originate or terminate on the affected Cisco device itself. It does not apply to TCP traffic that is merely forwarded through the device.**

## Software Versions and Fixes

The following table summarizes the 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 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 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 IOS release names and abbreviations is available at <http://www.cisco.com/warp/public/620/1.html>.

Train	Description of Image or Platform	Availability of Fixed Releases*		
11.0-based Releases		Rebuild	Interim**	Maintenance
11.0	Major release for all platforms	11.1(22a) 2001-Mar-19		
11.1-based Releases		Rebuild	Interim**	Maintenance
11.1	Major release for all platforms	11.1(24a) 2001-Mar-19		
11.1AA	ED release for access servers: 1600, 3200, and 5200 series.	Unavailable		
		Upgrade recommended to 12.1(7), available		
11.1CA	Platform-specific support for 7500, 7200, 7000, and RSP	11.1(35)CA26 2001-Mar-19		
11.1CC		11.1(36)CC1 2001-Mar-02		

	ISP train: added support for FIB, CEF, and NetFlow on 7500, 7200, 7000, and RSP	2001-Mar-02		
11.1CT	Added support for Tag Switching on 7500, 7200, 7000, and RSP	12.0(11)ST2		
11.1IA	Distributed Director only	2001-Feb-26 11.1(28a)IA1		
		2001-Mar-02		
11.2-based Releases		Rebuild	Interim**	Maintenance
11.2	Major release, general deployment	11.2(25a)		11.2(25)
11.2BC	Platform-specific support for IBM networking, CIP, and TN3270 on 7500, 7000, and RSP	2001-Mar-05 Unavailable		Available
11.2F	Feature train for all platforms	2001-Feb-26 Unavailable		Available
11.2GS	Early deployment release to support 12000 GSR	Unavailable		Upgrade recommended to 12.0(15)S1, available
11.2P	New platform support	2001-Feb-26 11.2(25a)P		11.2(25)P
		2001-Mar-05		Available
11.2SA	Catalyst 2900XL switch only	Unavailable		Upgrade recommended to 12.0WC
11.2WA3	LightStream 1010 ATM switch		12.0(10)W(18b)	12.0(13)W5(19b)
			Available	Available
11.2(4)XA	Initial release for the 1600 and 3600	11.2(25a)P		11.2(25)P
		2001-Mar-05		Available
11.2(9)XA	Initial release for the 5300 and digital modem support for the 3600	11.2(25a)P		11.2(25)P
11.3-based Releases		2001-Mar-05 Rebuild	Interim**	Available Maintenance
11.3	Major release for all platforms	11.3(11b)		

		2001-Mar-05		
11.3AA	ED for dial platforms and access servers: 5800, 5200, 5300, 7200	11.3(11a)AA		
11.3DA	Early deployment train for ISP DSLAM 6200 platform	2001-Mar-05 Unavailable		
11.3DB	Early deployment train for ISP/Telco/PTT xDSL broadband concentrator platform, (NRP) for 6400	Upgrade recommended to 12.1(5)DA1, available 2001-Mar-19		
11.3HA	Short-lived ED release for ISR 3300 (SONET/SDH router)	2001-Feb-28  Vulnerable		
11.3MA	MC3810 functionality only	11.3(1)MA8  2001-Mar-19		
11.3NA	Voice over IP, media convergence, various platforms	Unavailable  Upgrade recommended to 12.1(7), available 2001-Feb-26		
11.3T	Early deployment major release, feature-rich for early adopters	2001-Feb-26		
11.3WA4	LightStream 1010	2001-Mar-05	12.0(10)W(18b) Available	12.0(13W5(19b)) Available
11.3(2)XA	Introduction of ubr7246 and 2600	11.3(11b)T1  2001-Mar-05		
<b>12.0-based Releases</b>		<b>Rebuild</b>	<b>Interim**</b>	<b>Maintenance</b>
12.0	General deployment release for all platforms			12.0(15)
12.0DA	xDSL support: 6100, 6200	Unavailable  Upgrade recommended to 12.1(5)DA1, available 2001-Mar-19		Available

12.0DB	General deployment release for all platforms	Unavailable		
12.0DC	General deployment release for all platforms	Upgrade recommended to 12.1(4)DB1, available 2001-Feb-28		
12.0S	Core/ISP support: GSR, RSP, c7200	2001-Feb-28	12.0(14.6)S	
		Available	Available	
12.0SC	Cable/broadband ISP:ubr7200	12.0(15)SC1		
		2001-Mar-05		
12.0SL	10000 ESR: c10k	12.0(14)SL1		
		2001-Feb-26		
12.0ST	General deployment release for all platforms	12.0(11)ST2		
12.0SX	Early Deployment (ED)	2001-Feb-26 12.0(5c)E8		
		2001-Feb-26		
12.0T	Early Deployment(ED): VPN, Distributed Director, various platforms	Unavailable		
		Upgrade recommended to 12.1(7), available		
12.0W5	Catalyst switches: cat8510c, cat8540c, ls1010, cat8510m, cat8540m	2001-Feb-26		12.0(13)W5(19c)
	Catalyst switches: cat5atm, cat2948g-L3, cat4232			2001-Mar-14 12.0(14)W5(20)
	Catalyst switches: c6msm			2001-Mar-02 12.0(13)W5(19c)
				2001-Mar-14
12.0WT	Catalyst switches: cat4840g	12.0(13)WT6(1)		
		2001-Mar-15		
12.0XA	Early Deployment (ED): limited platforms	Unavailable		
		Upgrade recommended to 12.1(7), available		
12.0XB	Short-lived early	2001-Feb-26	Unavailable	

	deployment release	Upgrade recommended to 12.1(7), available 2001-Feb-26		
12.0XC	Early Deployment (ED): limited platforms	Unavailable		
		Upgrade recommended to 12.1(7), available		
12.0XD	Early Deployment (ED): limited platforms	2001-Feb-26 Unavailable		
		Upgrade recommended to 12.1(7), available		
12.0XE	Early Deployment (ED): limited platforms	2001-Feb-26 Unavailable		
		Upgrade recommended to 12.1(5)E8, available		
12.0XF	Early Deployment (ED): limited platforms	2001-Mar-05 Unavailable		
		Upgrade recommended to 12.1(7), available		
12.0XG	Early Deployment (ED): limited platforms	2001-Feb-26 Unavailable		
		Upgrade recommended to 12.1(7), available		
12.0XH	Early Deployment (ED): limited platforms	2001-Feb-26 12.0(4)XH5		
12.0XI	Early Deployment (ED): limited platforms	2001-Mar-12 Unavailable		
		Upgrade recommended to 12.1(7), available		
12.0XJ	Early Deployment (ED): limited platforms	2001-Feb-26 Unavailable		
		Upgrade recommended to 12.1(7), available		
12.0XK	Early Deployment (ED): limited platforms	2001-Feb-26 12.0(7)XK4		
12.0XL	Early Deployment (ED): limited platforms	2001-Mar-26 12.0(4)XH5		
				12.1(7)
12.0XM	Early Deployment (ED): limited platforms	2001-Mar-12 12.0(5)XM1		
12.0XN	Early Deployment (ED): limited platforms	2001-Mar-05		
12.0XP	Early Deployment (ED): limited platforms	Unavailable		
		Upgrade recommended to 12.1WC, available 2001-APR-12		

12.0XQ	Short-lived early deployment release	Unavailable		
		Upgrade recommended to 12.1(7), available		
12.0XR	Short-lived early deployment release	2001-Feb-26 Unavailable		
		Upgrade recommended to 12.1(5)T5, available		
12.0XS	Short-lived early deployment release	2001-Mar-05 Unavailable		
		Upgrade recommended to 12.1(5)E8, available		
12.0XU	Early Deployment (ED): limited platforms	2001-Mar-5 Unavailable		
		Upgrade recommended to 12.1WC, available		
12.0XV	Short-lived early deployment release	2001-APR-12 Unavailable		
		Upgrade recommended to 12.1(5)T5, available		
12.1-based and Later Releases		2001-Mar-05 Rebuild	Interim**	Maintenance
12.1	General deployment release for all platforms	12.1(5c)		12.1(7)
12.1AA	Dial support	2001-Feb-20		Available 12.1(7)AA
				2001-Mar-12
12.1DA	xDSL support: 6100, 6200	12.1(5)DA1		12.1(6)DA
		2001-Feb-28		2001-Feb-26
12.1CX	Core/ISP support: GSR, RSP, c7200			12.1(4)CX
				2001-Mar-13
12.1DB	General deployment release for all platforms	12.1(4)DB1		12.1(5)DB
12.1DC	General deployment release for all platforms	2001-Mar-05 12.1(4)DC2		2001-Mar-19 12.1(5)DC
12.1E	Core/ISP support: GSR, RSP, c7200	2001-Mar-05 12.1(5c)E8		2001-Mar-19 12.1(6)E
		2001-Mar-5		2001-Mar-12
12.1EC	Core/ISP support: GSR, RSP, c7200	12.1(5)EC1		12.1(6)EC
		2001-Feb-26		2001-Mar-26
12.1EX	Core/ISP support: GSR, RSP, c7200	12.1(5c)EX		
		2001-Mar-12		

12.1EY	Cat8510c, Cat8510m, Cat8540c, Cat8540m, LS1010	Not Vulnerable		
12.1T	Early Deployment(ED): VPN, Distributed Director, various platforms	12.1(5)T5		
12.1XA	Early Deployment (ED): limited platforms	2001-Mar-05 12.1(5)T5		
12.1XB	Early Deployment (ED): limited platforms	2001-Mar-05 12.1(5)T5		
12.1XC	Early Deployment (ED): limited platforms	2001-Mar-05 12.1(5)T5		
12.1XD	Early Deployment (ED): limited platforms	2001-Mar-05 12.1(5)T5		
12.1XE	Early Deployment (ED): limited platforms	2001-Mar-05 12.1(5)T5		
12.1XF	Early Deployment (ED): 811 and 813 (c800 images)	2001-Mar-05 12.1(2)XF3		
12.1XG	Early Deployment (ED): 800, 805, 820, and 1600	2001-Mar-05 12.1(3)XG3		
12.1XH	Early Deployment (ED): limited platforms	Available 12.1(2)XH5		
12.1XI	Early Deployment (ED): limited platforms	2001-Mar-12 12.1(3a)XI6		
12.1XJ	Early Deployment (ED): limited platforms	2001-Mar-19		Indeterminate
12.1XK	Early Deployment (ED): limited platforms	12.1(5)T5		Unscheduled
12.1XL	Early Deployment (ED): limited platforms	2001-Mar-05 12.1(3)XL1		

2001-Mar-05

12.1XM	Short-lived early deployment release	12.1(5)XM1		
12.1XP	Early Deployment (ED): 1700 and SOHO	<del>2001-Feb-28</del> 12.1(3)XP3		
12.1XQ	Short-lived early deployment release	<del>2001-Mar-05</del> 12.1(3)XQ3		
12.1XR	Short-lived early deployment release	<del>2001-Mar-12</del> 12.1(5)XR1		
12.1XS	Short-lived early deployment release	2001-Feb-20		12.1(5)XS
12.1XT	Early Deployment (ED): 1700 series	12.1(3)XT1		2001-Mar-12
12.1XU	Early Deployment (ED): limited platforms	Available 12.1(5)XU1		
12.1XV	Short-lived early deployment release	<del>2001-Feb-15</del> 12.1(5)XV1		
12.1XW	Short-lived early deployment release	<del>2001-Mar-12</del> 12.1(5)XW2		
12.1XX	Short-lived early deployment release	<del>2001-Mar-06</del> 12.1(5)XX3		
12.1XY	Short-lived early deployment release	<del>2001-Mar-06</del> 12.1(5)XY4		
12.1XZ	Short-lived early deployment release	<del>2001-Mar-06</del> 12.1(5)XZ2		
12.1YA	Short-lived early deployment release	<del>2001-Mar-06</del> 12.1(5)YA1		
12.1YB	Short-lived early deployment release	2001-Mar-06		12.1(5)YB
12.1YC	Short-lived early deployment release	12.1(5)YC1		2001-Feb-13

2001-Feb-26

12.1YD	Short-lived early deployment release			12.1(5)YD
Notes				2001-Mar-12
<p>* All dates are estimated and subject to change.</p> <p>** Interim releases are subjected to less rigorous testing than regular maintenance releases, and may have serious bugs.</p>				

## Workarounds

There is no specific configurable workaround to directly address the possibility of predicting a TCP Initial Sequence Number. To prevent malicious use of this vulnerability from inside the network, ensure that transport that makes interception and modification detectable, if not altogether preventable, is in use as appropriate. Examples include using IPSEC or SSH to the Cisco device for interactive session, MD5 authentication to protect BGP sessions, strong authentication for access control, and so on.

Malicious use of this vulnerability from a position outside the administrative boundaries of the network can be mitigated, if not prevented entirely, by using access control lists to prevent the injection of packets with forged source or destination IP addresses.

## Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

## Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

## Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and

releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

## Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

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

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

## Exploitation and Public Announcements

The general case of this vulnerability in TCP is well-known to the information system security community. Details specific to TCP connections to or from Cisco products do not appear to be widely known and the topic does not appear to have been widely discussed.

Cisco is not aware of instances in which this vulnerability has been used maliciously. However, there are numerous off-the-shelf programs and scripts available which can demonstrate the vulnerability and which could be modified to exploit it with malicious intent. Various security scanning programs have been known to provide positive test results for this vulnerability on Cisco devices.

This vulnerability was discovered internally. Two customers reported the vulnerability while a fix was still in progress.

## Status of This Notice: INTERIM

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. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

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 at

<http://www.cisco.com/warp/public/707/cisco-sa-20010301-ios-tcp-isn-random.shtml>.

In addition to Worldwide Web posting, a text version of this notice will be clear-signed with the Cisco PSIRT PGP key and will be posted to the following e-mail and Usenet news recipients:

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- Various internal Cisco mailing lists

Future updates of this notice, 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 URL given above for any updates.

## Revision History

Revision 1.3	2004-January-07	Corrected typo in software table for IOS 11.2SA
Revision 1.2	2001-March-07	Revised software tale with correct version numbers
Revision 1.1	2001-March-02	Revised software table with correct version numbers
Revision 1.0	2001-March-01	Initial public release

## Cisco Security Procedures

The page 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) contains instructions for reporting security vulnerabilities in Cisco products, obtaining assistance with customer security incidents, registering to receive security information from Cisco, and making press inquiries regarding Cisco Security Advisories. This document is Cisco's complete public statement regarding this product security vulnerability.

---

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

---

Updated: Jan 07, 2004

Document ID: 13631

---