

# Cisco Security Advisory: IOS Reload after Scanning Vulnerability

Document ID: 13632

Advisory ID: cisco-sa-20010524-ios-tcp-scanner-reload

<http://www.cisco.com/warp/public/707/cisco-sa-20010524-ios-tcp-scanner-reload>

## Revision 1.1

For Public Release 2001 May 24 1600 UTC (GMT)

---

Please provide your feedback on this document.

---

**Summary**  
**Affected Products**  
**Details**  
**Impact**  
**Software Versions and Fixes**  
**Workarounds**  
**Obtaining Fixed Software**  
**Exploitation and Public Announcements**  
**Status of This Notice: FINAL**  
**Distribution**  
**Revision History**  
**Cisco Security Procedures**

---

## Summary

Security Scanning software can cause a memory error in Cisco IOS® Software that will cause a reload to occur. This vulnerability affects only Cisco IOS software version 12.1(2)T and 12.1(3)T, and limited deployment releases based on those versions.

Customers using the affected Cisco IOS software releases are urged to upgrade as soon as possible to later versions that are not vulnerable to this defect. Vulnerable products and releases are listed in detail below.

The security scanner makes TCP connection attempts to various ports, looking for open ports to further investigate known vulnerabilities with those services associated with certain ports. However, a side effect of the tests exposes the defect described in this security advisory, and the router will reload unexpectedly as soon as it receives a request to review or write the configuration file.

This defect is documented as Cisco Bug ID CSCds07326.

The complete notice will be available at  
<http://www.cisco.com/warp/public/707/cisco-sa-20010524-ios-tcp-scanner-reload.shtml>.

# Affected Products

This section provides details on affected products.

## Vulnerable Products

It is impossible to list all Cisco products in this notice; the lists below include only the most commonly used or most asked-about products.

If you are unsure whether your device is running Cisco IOS software, log into the device and issue the command **show version**. Cisco IOS software will identify itself simply as "IOS" or "Internetwork Operating System Software". Other Cisco devices either will not have the **show version** command, or will give different output.

Cisco devices that run Cisco IOS software include the following:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 8xx,ubr9xx, 1xxx, 25xx, 26xx, 30xx, 36xx, 38xx, 40xx, 45xx, 47xx, AS52xx,
- AS53xx, AS58xx, 64xx, 70xx, 72xx (including theubr72xx), 75xx, and 12xxx series.
- Most recent versions of the LS1010 ATM switch.
- Some versions of the Catalyst 2900XL LAN switch.
- The Cisco DistributedDirector.

The affected software versions are relatively new, and are not necessarily available on every device listed above.

## Products Confirmed Not Vulnerable

If you are not running Cisco IOS software, you are not affected by this vulnerability. Cisco devices which do not run Cisco IOS software, and are not affected by this vulnerability, include the following:

- 7xx dialup routers (750, 760, and 770 series) are not affected.
- Catalyst 19xx, 28xx, 29xx, 3xxx, and 5xxx LAN switches are not affected, except for some versions of the Catalyst 2900XL. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, are affected.
- WAN switching products in the IGX and BPX lines are not affected.
- The MGX (formerly known as the AXIS shelf) is not affected.
- No host-based software is affected.
- The Cisco PIX Firewall is not affected.
- The Cisco LocalDirector is not affected.
- The Cisco Cache Engine is not affected.
- The Cisco CSS 11000 series switch is not affected

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

## Details

An attempt to make a TCP connection to ports 3100–3999, 5100–5999, 7100–7999, and 10100–10999 will cause the router to unexpectedly reload at the next **show running-config**, or **write memory**, or any command that causes the configuration file to be accessed. Cisco IOS software cannot be configured to support any services that might listen at those port addresses, and cannot be configured to accept connections on those

ports, however, connection attempts to these ports in the affected version will cause memory corruption, later leading to an unexpected reload.

Software packages are available from various commercial and free sites that perform automated remote tests for computer security vulnerabilities by scanning computers on a network for known security flaws. A common log message in environments that experienced security scan related crashes was the "attempt to connect to RSHELL" error message.

- **Bug ID** --- This problem was introduced in 12.1(1.3)T, and is identified by Cisco Bug ID CSCds07326.

## Impact

The described defect can be used to mount a denial of service (DoS) attack on any vulnerable Cisco product, which may result in violations of the availability aspects of a customer's security policy. This defect by itself does not cause the disclosure of confidential information nor allow unauthorized access.

## Software Versions and Fixes

This defect was introduced in version 12.1(1.3)T, and is repaired in the following versions which are based on the 12.1(2)T and 12.1(3)T releases.

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

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

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

- **Maintenance**  
Most heavily tested and highly recommended release of any label in a given row of the table.
- **Rebuild**  
Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific defect. Although it receives less testing, it contains only the minimal changes necessary to effect the repair.
- **Interim**  
Built at regular intervals between maintenance releases and receive less testing. Interims should be selected only if there is no other suitable release that addresses the vulnerability, and interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available via manufacturing, and usually they are not available for customer download from CCO without prior arrangement with the Cisco TAC.

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

<http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm>. In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco TAC for assistance as shown later in this notice.

More information on Cisco IOS Software release names and abbreviations is available at [http://www.cisco.com/en/US/products/sw/iosswrel/tsd\\_products\\_support\\_category\\_home.html](http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html).

Major Release	Description	Availability of Repaired Releases*		
		Rebuild	Interim**	Maintenance
Unaffected Earlier Releases	or Platform			
12.0 and earlier, all variants	Numerous	Not vulnerable	Not vulnerable	Not vulnerable
12.1-based Releases		vulnerable Rebuild	vulnerable Interim**	vulnerable Maintenance
12.1	General Deployment (GD) candidate: all platforms	Not vulnerable	Not vulnerable	Not vulnerable
12.1AA	Dial Support	Not vulnerable	Not vulnerable	Not vulnerable
12.1CX	Core/ISP support: GSR, RSP, C7200	Not vulnerable	Not vulnerable	Not vulnerable
12.1DA	xDSL Support: 6100, 6200	Not vulnerable	Not vulnerable	Not vulnerable
12.1DB	Cisco 6400 Universal Access Concentrator			12.1(4)DB
12.1DC	xDSL NRP support: c6400r			12.1(4)DC
12.1E	Core/ISP Support: GSR, RSP, c7200	Not vulnerable	Not vulnerable	Not vulnerable
12.1EC	Early Deployment (ED): ubr7200, UBR	Not vulnerable	Not vulnerable	Not vulnerable

	Headend platforms			
12.1EX	Catalyst 6000	Not vulnerable	Not vulnerable	Not vulnerable
12.1EY	Catalyst 8510, 8540, LS1010	Not vulnerable	Not vulnerable	Not vulnerable
12.1T	New technology Early Deployment (ED): all platforms		12.1(4.3)T	12.1(5)T
12.1XA	Early Deployment (ED): limited platforms	Not vulnerable	Not vulnerable	Not vulnerable
12.1XB	Early Deployment (ED): limited platforms			12.2(1)
12.1XC	Early Deployment (ED): limited platforms			12.2(1)
12.1XD	Early Deployment (ED): limited platforms	Not vulnerable	Not vulnerable	Not vulnerable
12.1XE	Early Deployment (ED): limited platforms			12.2(1)
12.1XF	Early Deployment (ED): limited platforms			12.2(1)
12.1XG	Early Deployment (ED): limited platforms			12.2T***
12.1XH	Early Deployment (ED): limited platforms			12.2(1)
12.1XI				12.2(1)

	Early Deployment (ED): limited platforms			
12.1XJ	Early Deployment (ED): limited platforms			12.2T***
12.1XK	Early Deployment (ED): limited platforms			12.2(1)
12.1XL	Early Deployment (ED): limited platforms			12.2(1)
12.1XM	Early Deployment (ED): limited platforms	Not Vulnerable	Not Vulnerable	Not Vulnerable
12.1XP	Early Deployment (ED): limited platforms			12.2T***
12.1XQ	Early Deployment (ED): limited platforms			12.2T***
12.1XR	Early Deployment (ED): limited platforms	Not Vulnerable	Not Vulnerable	Not Vulnerable
12.1XS	Early Deployment (ED): limited platforms			12.1(5)XS
12.1XT	Early Deployment (ED): limited platforms			12.2T***
12.1XU	Early Deployment (ED): limited platforms	Not Vulnerable	Not Vulnerable	Not Vulnerable
12.1XV	Early Deployment (ED): limited	Not Vulnerable	Not Vulnerable	Not Vulnerable

	platforms			
12.1XW	Early Deployment (ED): limited platforms	Not Vulnerable	Not Vulnerable	Not Vulnerable
12.1XX	Early Deployment (ED): limited platforms	Not Vulnerable	Not Vulnerable	Not Vulnerable
12.1XY	Early Deployment (ED): limited platforms	Not Vulnerable	Not Vulnerable	Not Vulnerable
12.1XZ	Early Deployment (ED): limited platforms	Not Vulnerable	Not Vulnerable	Not Vulnerable
12.1YA	Early Deployment (ED): limited platforms	Not Vulnerable	Not Vulnerable	Not Vulnerable
12.1YB	Early Deployment (ED): limited platforms	Not Vulnerable	Not Vulnerable	Not Vulnerable
12.1YC	Early Deployment (ED): limited platforms	Not Vulnerable	Not Vulnerable	Not Vulnerable
12.1YD	Early Deployment (ED): limited platforms	Not Vulnerable	Not Vulnerable	Not Vulnerable
Notes				
<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> <p>*** This release does not have a rebuild solution. Customers should upgrade to 12.2T when it becomes available. This is not a misprint.</p>				

## Workarounds

This vulnerability can be mitigated by configuring access lists and applying access groups on all interfaces or on external devices or firewalls to prevent connection attempts to affected routers, and to eliminate router

addresses in any planned security scanning exercises.

## 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](mailto: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 Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory. However, many reports of reloads related to this vulnerability have been reported by customers, due to customer use of security scanning software.

## Status of This Notice: FINAL

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

## Distribution

This notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20010524-ios-tcp-scanner-reload.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)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [firewalls@lists.gnac.com](mailto:firewalls@lists.gnac.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 advisory, if any, will be placed on Cisco's Worldwide Web site, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

## Revision History

Revision 1.1	2001-May-24	Made changes to the workarounds section
Revision 1.0	2001-May-24	Initial public release.

## Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's Worldwide Web site at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices.

---

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

---

Updated: May 24, 2001

Document ID: 13632

---