

Cisco Security Advisory: Cisco IOS Remote Router Crash

Document ID: 13658

Advisory ID: cisco-sa-19980810-ios-login

<http://www.cisco.com/warp/public/707/cisco-sa-19980810-ios-login.shtml>

Revision 1.4

Last Updated 1998 August 20 0130 UTC (GMT)

For Public Release 1998 August 10 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

An error in Cisco IOS software makes it possible for untrusted, unauthenticated users who can gain access to the login prompt of a router or other Cisco IOS device, via any means, to cause that device to crash and reload.

This applies only to devices running classic Cisco IOS software, including most, but not all, Cisco router products. The easiest way to determine whether your device is running classic Cisco IOS software is to use the **show version** command as detailed under [Who Is Affected](#) below.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19980810-ios-login.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

All users of classic Cisco IOS software versions 9.1 and later, but earlier than the repaired versions listed in the "[Details](#)" section of this notice, whose devices can be connected to interactively by untrusted users, are affected by this vulnerability. It is not necessary to be able to actually log in to exploit this vulnerability; simply establishing a terminal connection is sufficient. The vulnerability can be exploited from any interactive prompt issued by the router, including but not limited to, the login prompt.

Note that some of the repaired software has been in the field for some time; you may already have installed it. Please check your software version number before assuming that you are affected.

The vulnerability can be exploited using direct console or asynchronous serial connections (including dialup connections), TELNET connections, UNIX "r" command connections, LAT connections, MOP connections, X.29 connections, V.120 connections, and possibly others. Except in extraordinary security environments, administrators are strongly encouraged to assume that hostile users can find ways to make interactive connections to their Cisco IOS devices.

It is impossible to list all Cisco products in this notice. If you are unsure whether your device is running classic Cisco IOS software, log into the device and issue the command **show version**. Classic Cisco IOS software will identify itself simply as "IOS" or "Internetwork Operating System Software," and affected software will have a version number greater than or equal to 9.1. Other Cisco devices either will not have the **show version** command, or will give different output.

Products Confirmed Not Vulnerable

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

- 7xx dialup routers (750, 760, and 770 series) are *not* affected.
- Catalyst LAN switches (except for the Catalyst 2900XL) are *not* affected.
- WAN switching products in the IGX or BPX lines are *not* affected.
- The AXIS shelf is *not* affected.
- The LS1010 or LS2020 ATM switches are *not* affected. Earlier versions of this notice said that some LS1010 switches were affected. This was an error; the 11.2WAx and 11.3WAx versions of Cisco IOS software used in LS1010 switches are based on repaired variants.
- Any host-based software is *not* vulnerable.
- The Cisco PIX Firewall is *not* vulnerable.
- The Cisco LocalDirector is *not* vulnerable.
- The Cisco Cache Engine is *not* vulnerable.

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

Details

The Cisco IOS software error has been assigned Cisco bug ID [CSCdj43337](#).

Note: If you are a [registered CCO user](#) and you have logged in, you can view bug details.

Impact

If attackers know the details of the Cisco IOS software error they will be able to cause the router to crash and reload *without having to log in to the router*. Because this problem involves damage to an internal data

structure, it is possible that other, more subtle or targeted effects on system operation could also be induced by proper exploitation. Such exploitation, if it is possible at all, would require significant engineering skill and a thorough knowledge of the internal operation of Cisco IOS software, including Cisco trade secret information.

Software Versions and Fixes

This vulnerability affects all releases of Classic Cisco IOS software from 9.1 up to, but not including, the following corrected releases (including interim and beta software):

- 11.3(1), 11.3(1)ED, 11.3(1)T
- 11.2(10), 11.2(9)P, 11.2(9)XA, 11.2(10)BC, 11.2(8)SA3
- 11.1(15)CA, 11.1(16), 11.1(16)IA, 11.1(16)AA, 11.1(17)CC, 11.1(17)CT
- 11.0(20.3)

It is not necessary to run the specific releases listed above; the fix is present in all subsequent versions of the same releases as well. For example, 11.2(9)P is fixed, so 11.2(10)P is also fixed.

Releases of Cisco IOS software up to and including 10.3 have reached end of support, and no fixes are currently or planned to be available for those releases. All releases after 9.1 do, however, contain the problem.

All planned fixes to Cisco IOS software have been completed and tested. Integration into regular released software is complete for all versions except 11.0. If you are running a version of software earlier than the ones listed above, please contact the Cisco TAC for assistance.

As of the date of this notice, the fix for this problem is available for the 11.0 release only in the 11.0(20.3) version. This is an interim release, and has not been subjected to the same degree of testing as a regular Cisco IOS release. The first regular 11.0 release containing the fix will be 11.0(21). Release of 11.0(21) is tentatively scheduled for mid-September, 1998; this schedule is subject to change. Because of the relative maturity of the 11.0 Cisco IOS software, Cisco believes that installation of 11.0(20.3) carries less risk than would installation of an interim release for a newer Cisco IOS version, but customers are advised to use caution in installing 11.0(20.3), or any other interim release, in any critical device.

Workarounds

It is possible to work around this problem by preventing interactive access to the Cisco IOS device. If only IP-based interactive access is of concern, this can be done by using the **ip access-class** line configuration to apply an access list to all virtual terminals in the system. However, it is important to remember that non-IP-based means of making interactive connections to Cisco IOS devices do exist, and to eliminate those means as possible routes of attack. Interactive access can be prevented completely by applying the configuration command **no exec** to any asynchronous line, or the command **transport input none** to any virtual terminal line, that may be accessible to untrusted users.

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

Cisco has had no actual reports of malicious exploitation of this vulnerability. However, there have been sporadic reports of unexplained crashes that have been consistent with the crashes caused by this vulnerability; the vulnerability was initially identified because of such a report. It is possible that the reported crashes could have been caused by random events, but it is also possible that they could have been deliberate. Cisco has essentially no information that would be useful in determining which is the case. None of the customers reporting the crashes indicated any suspicion of a deliberate attack.

Cisco knows of no public announcements of this vulnerability before the date of this notice.

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-19980810-ios-login.shtml>. In addition to Worldwide Web posting, the initial version of this notice is being sent to the following e-mail and Usenet news recipients:

- cust-security-announce@cisco.com
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- first-info@first.org
- Various internal Cisco mailing lists

Future updates of this advisory, 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 above URL for any updates.

Revision History

Revision 1.4	1998-August-20	Error with respect to impact on LS1010 switches corrected. 11.2(8)SA3 added to repaired version list.
Revision 1.3	1998-August-19	Various common misunderstandings corrected. More information about which Cisco IOS software versions are vulnerable and about which products run classic Cisco IOS software.
Revision 1.2	1998-August-10	Initial public release.

Cisco Security Procedures

Please report security issues with Cisco products, and/or sensitive security intrusion emergencies involving Cisco products, to security-alert@cisco.com. Reports may be encrypted using PGP; public RSA and DSS keys for "security-alert@cisco.com" are on the public PGP keyservers.

The alias "security-alert@cisco.com" is used only for reports incoming to Cisco. Mail sent to the list goes only to a very small group of users within Cisco. Neither outside users nor unauthorized Cisco employees may subscribe to "security-alert@cisco.com".

Please do not use "security-alert@cisco.com" for configuration questions, for security intrusions that you do not consider to be sensitive emergencies, or for general, non-security-related support requests. We do not have the capacity to handle such requests through this channel, and will refer them to the TAC, delaying response to your questions. We advise contacting the TAC directly with these requests. TAC contact numbers 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

All formal public security notices generated by Cisco are sent to the public mailing list "cust-security-announce@cisco.com". For information on subscribing to this mailing list, send a message containing the single line "info cust-security-announce" to "majordomo@cisco.com". An analogous list, "cust-security-discuss@cisco.com" is available for public discussion of the notices and of other Cisco security issues.

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

Updated: Aug 20, 1998

Document ID: 13658
