

Cisco Security Advisory: Cisco IOS Command History Release at Login Prompt

Document ID: 13657

Advisory ID: cisco-sa-19981014-ios-hist

<http://www.cisco.com/warp/public/707/cisco-sa-19981014-ios-hist.shtml>

Revision 1.0

For Public Release 1998 October 14 1500 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 obtain fragments of text entered by prior interactive users of the device. This text may contain sensitive information, possibly including passwords. This vulnerability exposes only text entered at prompts issued by the IOS device itself; the contents of data packets forwarded by IOS devices are not exposed, nor are data entered as part of outgoing interactive connections, such as TELNET connections, from the IOS device to other network nodes.

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.

Although the conditions under which it can be exploited are similar, this vulnerability is not related to the remote crash vulnerability announced in August, 1998.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19981014-ios-hist.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. Note that all of the repaired versions are quite recent as of the date of this notice, and that it is unlikely that most Cisco users have installed them. The vulnerability affects the vast majority of systems running Cisco IOS software as of this date.

The vulnerability can be exploited using direct console or asynchronous serial connections (including dialup connections), TELNET connections, UNIX "r" command connections, local-area transport (LAT) connections, Maintenance Operation Protocol (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 not necessary to be able to actually log in to exploit this vulnerability; simply establishing a terminal connection is sufficient.

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

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". Other Cisco devices either will not have the **show version** command, or will give different output.

Cisco devices that run classic Cisco IOS software include:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 8xx, 1xxx, 25xx, 26xx, 30xx, 36xx, 40xx, 45xx, 47xx, AS52xx, AS53xx, 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

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, 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.

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

Details

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

- View [CSCdk43920](#)

Impact

If attackers know the details of the Cisco IOS software error, they will be able to obtain fragments of the last few lines of text entered in response to IOS prompts on the physical or virtual TTYs to which they are connected. The exact amount of recoverable text varies, and will be split among fragments of various lines. Nearly complete lines, and fragments tens of characters long, can sometimes be obtained.

If the previous session was brief, the available information may include part or all of the password that a previous user used to log into the router or to enable privileged mode. If a previous user changed a system password, such as the enable password, and logged out shortly thereafter, it may be possible to recover the new password by reading the configuration command used to make the change.

This vulnerability does not expose anything entered as part of an outgoing session from the IOS device to another node. For example, if a user logs into an IOS router, and then makes a TELNET connection to a remote host, none of the data in the TELNET connection itself can be recovered.

Software Versions and Fixes

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

Earliest Regular Releases	Earliest Interim Releases
11.0(22)	11.0(21.2)
11.1(22), 11.1(22)CA, 11.1(21)CC1, 11.1(22)CE	11.1(22), 11.1(21.2)CA, 11.1(21)CC1, 11.1(21.1)CE
11.2(16), 11.2(16)P, 11.2(16)BC, 11.2(8)SA4	11.2(15.4), 11.2(15.4)P, 11.2(15.4)BC, 11.2(8)SA4
11.3(6), 11.3(6)T, 11.3(6)AA, 11.3(1)MA6, 11.3(6)NA, 11.3(9)WA4	11.3(5.6), 11.3(5.6)T, 11.3(5.6)AA, 11.3(1)MA54, 11.3(5.6)NA
12.0(1), 12.0(1)T, 12.0(1)S, other 12.0	Will be integrated in initial 12.0(1)x releases

It is not necessary to run the specific versions listed above; the fix is present in all subsequent versions of the same releases as well. For example, 11.2(16)P is fixed, so 11.2(17)P will also be fixed.

The fix is available in all regular releases as of the date of this notice. However, the fix has not yet been released for all "two-letter" early deployment software. Integration is under way for the unreleased "two-letter" versions.

Some releases of Cisco IOS software have been obsoleted or have reached end of maintenance. The upgrade paths for the users of these releases are as follows:

Obsolete Release	Upgrade To
1.x – 8.x, 9.1, 9.14, 9.17, 9.21, 10.1, 10.2, 10.3 (all variants)	11.0 (be especially careful to check hardware compatibility)
11.0BT	11.1
11.1AA	11.2(16)P
11.2(4)XA, 11.2(9)XA	11.2(16)P
11.3(2)XA	11.3(3)
11.2F	11.3(6)

Workarounds

There are two major workarounds for this vulnerability:

1. Prevent untrusted users from having interactive access to the Cisco IOS device. If only IP-based interactive access is of concern, access can be restricted by using the **ip access-class** line configuration command 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. The **transport input** command is particularly useful in controlling the protocols that can be used to get interactive access. 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.
2. Overwrite any potentially sensitive information before logging out of any interactive session on an IOS device. This can be done by entering repeated spaces at an IOS command prompt until the command interpreter will accept no more input on the line, then pressing the "return" key. Follow this by entering a printing character, such as "q", repeatedly until no more input is accepted, then pressing control-A, followed by control-K, then "return" again. This procedure vastly reduces the probability of information leakage, but has not been verified to completely eliminate the possibility in all affected versions of Cisco IOS software.

Cisco recommends installing upgraded software in preference to using either of these workarounds. The first workaround should be part of normal security configuration in any Cisco IOS device, but cannot usually be used to eliminate all possible risk, since some interactive access must be available for system management. The second workaround is prone to human error, and, although it greatly reduces the probability of an attacker's finding anything sensitive, it does not completely eliminate that possibility.

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 knows of no public announcements or discussion of the details of this vulnerability prior to the date of this notice. An inadvertent preannouncement was made to certain Cisco customers during the week of October 5, but the *only* information given to those customers consisted of the bug ID and the bug headline, which was "Security Problem". In other words, they were told that a security problem existed in a version of Cisco IOS software, but were given absolutely no details. A later message to those same customers informed them that the vulnerability had been found by a trusted customer, that Cisco knew of no exploitation of the vulnerability, and that a formal notice would be forthcoming. Extreme care was taken to avoid giving information that could be used to localize the vulnerability to any particular part of the Cisco IOS software, or other information that might be useful in finding the details.

Cisco knows of no malicious exploitation of this vulnerability. This vulnerability was found by a Cisco customer during laboratory testing.

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-19981014-ios-hist.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
- fib-beta@external.cisco.com
- Various internal Cisco mailing lists

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 1.0	1998 October 14	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 key servers.

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: Oct 14, 1998

Document ID: 13657
