

Cisco Security Advisory: Cisco IOS 11.3(1.2) and 11.3(1.2)T AAA Failure

Document ID: 13649

Advisory ID: cisco-sa-19980122-aaapair

<http://www.cisco.com/warp/public/707/cisco-sa-19980122-aaapair.shtml>

Revision 3.0

For Public Release 1998 January 22 0000 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

A vulnerability (bug ID CSCdj74723) in AAA authentication processing on Cisco IOS versions 11.3(1.2) and 11.3(1.2)T may allow users to get access for which they are not intended to be authorized. This affects only the 11.3(1.2) and 11.3(1.2)T interim releases. It does not affect any non-interim, production Cisco IOS software release.

The bug that creates this vulnerability may also result in access being denied to legitimate users, or in system crashes. If you are a [registered CCO user](#) and you have logged in, you can view bug details.

[View CSCdj74723](#) ([registered](#) customers only)

The complete text of this advisory will be located at

<http://www.cisco.com/warp/public/707/cisco-sa-19980122-aaapair.shtml>

Affected Products

Vulnerable Products

All systems running Cisco IOS Software version 11.3(1.2) or 11.3(1.2)T, and which use TACACS+, RADIUS, or other AAA services for authorization, are affected by this vulnerability. If your configuration

includes any command beginning with "aaa authorization", then you are vulnerable. Systems using AAA strictly for login authentication, as opposed to service authorization, and systems using local authentication, are unaffected.

We believe that the most commonly affected configurations will be those using TACACS+ or RADIUS servers.

Systems running engineering special releases containing the fix for bug ID CSCdi51915 may also be affected. If you are a [registered CCO user](#) and you have logged in, you can view bug details.

[View CSCdi51915](#) ([registered](#) customers only)

Products Confirmed Not Vulnerable

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

Details

This vulnerability (Bug ID CSCdj74723) was introduced by the fix for Bug ID CSCdi51915, which was integrated in Cisco IOS versions 11.3(1.2) and 11.3(1.2)T. It has been fixed for 11.3(1.3) and 11.3(1.3)T. Only these interim releases are affected; CSCdj74723 is not in any regular, released Cisco IOS software image.

Cisco's product security incident response team does not know of any engineering specials that are vulnerable, but, because such specials may be released on an informal basis, it is impossible to determine with absolute certainty whether or not such images exist. Cisco personnel who have been involved in the issuance of specials to customers since January 8, 1998, and customers who have received such specials, are advised to check to make sure that the fix for CSCdi51915 is not in their specials. If that fix is there, the fix for CSCdj74723 must be added to protect against this vulnerability.

Impact

This vulnerability may let attackers evade authorization, which may mean that they can issue system commands that they would not otherwise be able to issue, or that they can make connections or send packets to destinations that they would not otherwise be able to reach. It is possible for this to happen without any special skills or knowledge on the part of the attacker, and it is also possible for extra access to be granted to a legitimate user who isn't deliberately conducting an attack at all. The effects of the vulnerability depend on the installation, but you should assume that it opens very broad access to your network.

The underlying bug can also result in denial of authorization to legitimate users, or in system crashes.

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.

Workarounds

There is no configuration workaround for this vulnerability, short of completely disabling AAA authorization.

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 known reports of malicious exploitation of this vulnerability.

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

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

The initial version of this notice is being sent to the customers that our records show have downloaded the affected releases.

This notice will be posted in the "[Field Notices](#)" section of Cisco's Worldwide Web site, which can be found under "Technical Tips" in the "Software and Support" section. The URL is <http://www.cisco.com/warp/public/707/cisco-sa-19980122-aaapair.shtml>. The copy on the Worldwide Web will be updated as appropriate.

If there are future changes to this notice, the new versions will be posted on the Worldwide Web. Updates will not be sent in e-mail unless the changes are significant.

Revision History

Revision 3.0	1998 JAN 21	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 security-alert@cisco.com 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. We will shortly be creating a security announcement mailing list for outgoing information. When that list is created, an announcement will be sent to appropriate Internet forums.

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 have to refer them to [Cisco's Technical Assistance Center](#), delaying response to your questions. We advise contacting the Technical Assistance Center directly with such questions.

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

Updated: Jan 21, 1998

Document ID: 13649
