

Cisco Security Advisory: Cisco CHAP Authentication Vulnerabilities

Document ID: 13652

Advisory ID: cisco-sa-19971001-chap

<http://www.cisco.com/warp/public/707/cisco-sa-19971001-chap.shtml>

Revision 4.0

For Public Release 1997 October 01 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

A serious security vulnerability (bug ID CSCdi91594) exists in PPP CHAP authentication in all "classic" Cisco IOS software versions (the software used on Cisco non-switch products with product numbers greater than or equal to 1000, on the AGS/AGS+/CGS/MGS, and on the CS-500, but not on Catalyst switches or on 7xx or 9xx routers) starting with the introduction of CHAP support in release 9.1(1). The vulnerability permits attackers with appropriate skills and knowledge to completely circumvent CHAP authentication. Other PPP authentication methods are not affected.

A related vulnerability exists in Cisco IOS/700 software (the software used on 7xx routers). A configuration workaround exists for IOS/700, and a complete fix for 76x and 77x routers will be included in software version 4.1(2), due to be released by December, 1997. A fix for 75x routers is scheduled for the first half of 1998.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19971001-chap.shtml>.

Affected Products

Vulnerable Products

All systems running "classic" Cisco IOS Software releases older than those listed above, and which rely on CHAP for PPP authentication, are vulnerable. Cisco believes that the greatest practical risk is to dial-in services that use, for example, ISDN or POTS modems.

Systems running IOS/700 software are vulnerable to a related attack if they are using CHAP bidirectionally to authenticate both calling and called systems. Systems using PAP for PPP authentication are not vulnerable.

Products Confirmed Not Vulnerable

Systems not configured for PPP are not vulnerable. If the keywords "ppp" and "chap" do not both appear in your system configuration file, you are not vulnerable.

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

Details

Cisco will not release any further details of these vulnerabilities at this time. Further details will be available to interested parties after March 31, 1998.

The Cisco bug tracking number for the Cisco IOS software vulnerability is CSCdi91594. The bug tracking number for the error in the 10.3(19) fix is CSCdj37314.

Impact

A moderately sophisticated programmer with appropriate knowledge can set up an unauthorized PPP connection to any system that is running vulnerable software, and that depends on CHAP for authentication. To gain this unauthorized access, an attacker must have the following:

- Knowledge of the details of this vulnerability
- Access to modifiable code (generally meaning source code) for a PPP/CHAP implementation, and sufficient programming skill to make simple changes to that code. Note that such source code is widely available on the Internet.
- A modest amount of information about the configuration of the network to be attacked, including such things as usernames and IP addresses.

This vulnerability cannot be exploited by an attacker who is using an unmodified, properly functioning PPP/CHAP implementation; the attacker must make modifications to his or her software to exploit this vulnerability.

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.

This problem has been corrected in the following classic Cisco IOS software releases:

Major Release	First Repaired	Recommended Maintenance
Cisco IOS 10.3	Maintenance Release 10.3(19a)	Releases For Installation 10.3(19a)
Cisco IOS 11.0	11.0(17), 11.0(17)BT	11.0(17), 11.0(17)BT
Cisco IOS 11.1	11.1(13), 11.1(13)AA, 11.1(13)CA, 11.1(13)IA	11.1(14), 11.1(14)AA, 11.1(14)CA, 11.1(14)IA
Cisco IOS 11.2	11.2(8), 11.2(8)P, 11.2(4)F1 (replaces 11.2(4)F)	11.2(8), 11.2(8)P, 11.2(4)F1. 11.2(9) not recommended for CHAP users.

Cisco Systems strongly recommends that all customers using classic Cisco IOS PPP with CHAP authentication upgrade to one of these or to a newer release, and that all users of IOS/700 PPP with CHAP authentication install the configuration workarounds described in this document.

The 11.2(4)F1 release will be available by Monday, October 6, 1997. Users of 11.2F releases are encouraged to move to 11.2 or 11.2P releases if at all possible. All the other releases mentioned above are available immediately as of the release of this notice.

The recommended release numbers listed above are expected to be the best choices for most common situations, but it's very important that customers evaluate their network configurations and other needs before choosing which releases to use.

Cisco is offering free software upgrades to all classic Cisco IOS PPP users in order to address this vulnerability. Upgrade details are at the end of this notice. Free upgrades will be offered to IOS/700 users upon release of IOS/700 version 4.1(2).

You should upgrade your classic Cisco IOS software to one of the releases mentioned in the first section of this notice, or to a later release. Instructions for obtaining the new software are at the end of this notice. Instructions for installing upgraded software are in the standard system documentation.

Before installing any Cisco IOS software upgrade, you should always verify that the new software is compatible with your hardware. It's especially important to make sure that you have enough memory to do the upgrade. General assistance and full system documentation are available via the Internet's Worldwide Web at <http://www.cisco.com>.

Before installing any upgrade of any description, it's always wise to make sure that the version you're installing has no bugs that will negatively impact your configuration. Please check Cisco's Web site for more information and advice on software upgrades in general.

The new software has been changed in a number of ways in order to make it more resistant to CHAP-related attacks. Some of those changes may cause CHAP authentication to fail in certain customer networks. Cisco believes the affected configurations to be rare. If you install upgraded software, and legitimate CHAP connections stop working, please see the paragraphs immediately following this one, which we believe describe the failures that are likely to be seen in real networks. If you still can't get CHAP working after

reading the paragraphs below, please call the Cisco TAC for assistance in reconfiguring your software.

The fix for this vulnerability was released in Cisco IOS software version 10.3(19), but an error in the implementation of the fix caused almost all CHAP authentication between 10.3(19) systems to fail. This error is corrected in 10.3(19a). 10.3(19) may be safely used if the command **no ppp chap wait** is configured for each interface on which CHAP is used. Because multiple fixes have been introduced for the potential attack against which the modified behavior guards, using **no ppp chap wait** will not appreciably increase your system's vulnerability.

If an intermediate device, such as an ISDN switch, establishes incoming calls to two separate systems running the modified Cisco IOS software, and then places those two systems in contact with one another, CHAP authentication between the two systems may fail. This is because each system "thinks" that it's receiving a call, and neither system "thinks" that it originated the call. If this is a problem in your configuration, use the command **ppp direction** dedicated on the affected interfaces of both systems.

Workarounds

This section describes workarounds for these vulnerabilities.

Classic Cisco IOS

Cisco knows of no generally usable workarounds for the classic Cisco IOS vulnerability. Affected users who wish to protect themselves must upgrade their software or stop using CHAP authentication. Alternatives to CHAP authentication include PAP authentication and reliance on "Caller ID" information. The security differences between these methods are complex and situation-dependent, and are beyond the scope of this document.

IOS/700

The IOS/700 vulnerability may be avoided by making any of the following configuration changes:

- Prevent the routers in question from receiving any incoming calls, perhaps by changing the ISDN switch configuration, or by relying on caller ID and using the **set callerid** and **set callidreceive** commands.
- Prevent routers that receive calls from authenticating themselves to the calling systems using CHAP. You can effectively do this by using the **set ppp secret client** command to set the CHAP secret that would be used for such authentication to some randomly chosen "garbage" value.
- Configure the routers such that different CHAP secrets are used in each direction on each link. You can do this using the **set ppp secret client** and **set ppp secret host** commands. Note that this method cannot be used on 7xx routers that need to communicate with classic Cisco IOS routers, because classic Cisco IOS does not support asymmetric CHAP secrets.

Any one of these changes should be sufficient. The changes may be removed after the release and installation of IOS/700 software version 4.1(2).

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 is not aware of these vulnerabilities having been exploited by "system crackers," nor of any publicly available exploitation code. Cisco does not believe that the details of the vulnerabilities are widely understood in the cracker community. The theoretical possibility of these vulnerabilities has, however, been discussed fairly openly among PPP security professionals.

Even though Cisco does not know of active exploitation of these vulnerabilities, Cisco expects that the cracker community will eventually "discover" them, and that the issuance of this notice will tend to accelerate that process. Vulnerable customers should upgrade or install workarounds with all possible speed.

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 advisory is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-19971001-chap.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
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

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 4.0	1997-October-01	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 website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.
