

Cisco Security Advisory: Incorrectly Parsed Access-list May Allow Packets to Bypass Filter

Document ID: 13606

Advisory ID: cisco-sa-19950731-acl-packet-bypass

<http://www.cisco.com/warp/public/707/cisco-sa-19950731-acl-packet-bypass.shtml>

Revision 1.0

For Public Release 1995 July 31 2324 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

The following describes an error in Cisco's IOS software 10.3 release when the 'tacacs-ds' or 'tacacs' keyword is used in extended IP access control lists.

The solution is to obtain and install the appropriate release of IOS software as described above. For assistance contact Cisco's TAC.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-19950731-acl-packet-bypass.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

This vulnerability is present in the following IOS software versions:

10.3(3.4) through 10.3(4.2)

If you are running any of these IOS versions on a product that uses IP extended access lists, and you are using the 'tacacs-ds' or 'tacacs' keyword in these lists, then Cisco strongly recommends that you review your access lists to insure that they have been parsed correctly. You can determine what version of IOS you are running by issuing the following command:

```
show version
```

If your access list has been parsed incorrectly, the recommended action is to upgrade to a more recent version of IOS or perform the workaround described below. The bug is fixed by in the following official software releases:

10.3(4.3) or later

(For reference, the Cisco update identifier for this fix is "CSCdi36962".)

Products Confirmed Not Vulnerable

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

Details

A bug in certain versions of IOS can cause extended IP access lists to be parsed incorrectly. Under some circumstances, this may allow packets to bypass IP packet filtering. This may permit unintended IP traffic to pass through a filtering router.

IP extended access lists between versions 10.3(1) through 10.3(3.3) used the keyword 'tacacs-ds'. This keyword could be saved as part of the router configuration either in non-volatile memory on the router or on an external TFTP server.

Configuration files written by these versions which are read by versions 10.3(3.4) through 10.3(4.2) will not have the 'tacacs-ds' keyword parsed correctly. The result will be that the entire line in the access list will be ignored. An error message will be generated when this occurs. Loss of such a line from the access list may create a vulnerability if the access list is used as part of a packet filter.

To determine if you are vulnerable, examine your current configuration and compare it to your intended configuration.

If the access lists in your current configuration and your intended configuration do not use the keyword 'tacacs-ds', you are not vulnerable. You do not need to do anything.

If your current configuration contains the keyword 'tacacs-ds', you should NOT upgrade that router to any version of IOS between 10.3(3.4) and 10.3(4.2). You are not currently vulnerable.

If your intended configuration contains the keywords 'tacacs-ds', 'tacacs', or filters on TCP or UDP port 49, and your current configuration does NOT contain this line of the access list, you are currently vulnerable. You should perform the workaround described below.

Impact

This bug can cause an extended IP access control list to be misparsed, possibly allowing unauthorized packets to circumvent a filtering router.

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.

Software upgrades may be obtained via any of the following mechanisms:

World Wide Web (WWW)

For registered CCO users please open a URL to:

<http://www.cisco.com/tacpage/sw-center/>

and select the the version of software to download.

For non-registered users open a URL to:

<https://www.cisco.com/cgi-bin/Software/SFA/sfa.cgi>

When prompted for a code, please enter:

```
certjuly31
```

for a list of available files to download.

FTP

ftp cco.cisco.com and at the initial (username) prompt, enter:

```
certjuly31
```

At the password prompt, enter your e-mail address. Then:

```
get README.certjuly31
```

This file contains a list of files available that close this vulnerability. Please examine this list to determine which files you need and then download them.

Character-based "CCO Classic"

For access, the following connection options are offered:

```
telnet cco.cisco.com
```

Dial-up modem

- In Europe +33 1 64 46 40 82
- In the US (408) 526 8070

vt100, N81, up to 14.4Kbps

Enter either as a guest or registered user and navigate to the topic:

```
Software Updates  
Special Files
```

At the prompt for a code, please enter:

```
certjuly31
```

A list of files will be displayed for you to select and download.

Workarounds

The following actions will remove the vulnerability:

Delete the access list and re-enter it based upon your intended configuration. Do not enter the 'tacacs-ds' keyword. Use the keyword 'tacacs' instead.

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/en/US/docs/general/warranty/English/EU1KEN.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/en/US/support/tsd_cisco_worldwide_contacts.html 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 vulnerability described in this advisory.

This vulnerability was reported to Cisco by .

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-19950731-acl-packet-bypass.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 1.0	1995-July-31	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>.

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jul 31, 1995

Document ID: 13606
