

Cisco Security Advisory: "Established" Keyword May Allow Packets to Bypass Filter

Document ID: 13607

Advisory ID: cisco-sa-19950601-key-packet-bypass

<http://www.cisco.com/warp/public/707/cisco-sa-19950601-key-packet-bypass.shtml>

For Public Release 1995 June 01 2337 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

This document describes a vulnerability in Cisco's IOS software when the 'established' keyword is used in extended IP access control lists. This bug can, under very specific circumstances and only with certain IP host implementations, allow unauthorized packets to circumvent a filtering router.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-19950601-key-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(1) through 10.3(2)

10.2(1) through 10.2(5)

10.0(1) through 10.0(9)

...and all previous versions of Cisco software.

If you are running any of these IOS versions on a product that uses IP extended access lists, and you are using the 'established' keyword in these lists, then Cisco strongly recommends that you take immediate action to remove the vulnerability. You can determine what version of IOS you are running by issuing the following command:

```
show version
```

Products Confirmed Not Vulnerable

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

Details

This section provides detailed information about these vulnerabilities.

Description

A bug in Cisco's extended IP access list implementation can, under very specific circumstances, allow a user to bypass IP packet filtering. This may permit unintended IP traffic to pass through your firewall setup.

To determine if you are vulnerable, look through your configuration. The configuration can be displayed by enabling and then entering the command "write term".

If you see an access list line using a list number in the range of 100 through 199 that permits or denies TCP traffic and contains the word 'established' near the end of the line, you may be vulnerable.

An example line might look like:

In IOS 10.3:

```
access-list 100 permit tcp any any established
```

In IOS 10.2 or earlier:

```
access-list 100 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0  
255.255.255.255 established
```

If you do not meet this test, then you are not vulnerable. You do not need to do anything.

Workaround

The following actions will remove the vulnerability:

- Rewrite the access list parameters so the 'established' keyword is not necessary. This does not simply mean that you may remove the 'established' keyword, but rather that you will need to re-design your access lists to provide similar functionality without using the established mechanism.

or

- Disable the interfaces to which the access list is applied using the 'shutdown' interface subcommand. Example:

```
router(config)#interface ethernet 0  
router(config-if)#shutdown
```

Solution

Obtain and install the appropriate release of IOS software as described above. For assistance, contact Cisco's TAC.

Technical Comments

This problem is caused by an obscure but common design flaw that we believe exists in many router/firewall vendor's packet filtering implementations.

Owners of non-Cisco hardware who use IP packet filtering features similar to Cisco's "extended access lists" as part of a firewall system may wish to contact their vendor to confirm that this vulnerability does not exist in their system. (Technical discussions about the problem have already occurred in the appropriate forum.)

This vulnerability can only be exploited with certain IP host implementations (we do not have information on which implementations are susceptible). Cisco suggests that all routers configured to filter IP packets based upon the 'established' mechanism be upgraded.

Impact

Successful exploitation of the vulnerability may, under very specific circumstances and only with certain IP host implementations, allow 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 the special access code you are given by your [Cisco Technical Assistance Center support representative](#) for a list of available files to download.

FTP

ftp cco.cisco.com and at the initial (username) prompt, enter the special access code you are given by your Cisco support representative as a userid. At the password prompt, enter your e-mail address.

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 the special access code you are given by your Cisco support representative for a list of available files to download. A list of files will be displayed for you to select and download.

Workarounds

The recommended action is to upgrade to a more recent version of IOS, or take one of the immediate workaround actions described below. The vulnerability is fixed by in the following official software releases:

```
10.0(10) or later
10.2(6) or later
10.3(3) or later
```

(For reference, the Cisco update identifier for this fix is "CSCdi34061".)

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-19950601-key-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-June-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>.

[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: Jun 01, 1995

Document ID: 13607
