

Cisco Security Advisory: Cisco IOS Software established Access List Keyword Error

Document ID: 13656

Advisory ID: cisco-sa-19990608-ios-grs-acl

<http://www.cisco.com/warp/public/707/cisco-sa-19990608-ios-grs-acl.shtml>

Revision 1.2

Last Updated 1999 June 08 1810 UTC (GMT)

For Public Release 1999 June 08 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

Cisco 12000 series Gigabit Switch Routers running certain versions of Cisco IOS software forward unauthorized traffic due to an error encountered while processing the **established** keyword in an **access-list** statement. The resulting vulnerability could be exploited to circumvent a site's security policy.

Only Cisco Gigabit Switch Routers (currently the 12008 and 12012 GSRs) running Cisco IOS software release 11.2(14)GS2 through 11.2(15)GS3 are vulnerable.

This error is corrected in release 11.2(15)GS5 and later versions.

This error is *not* present in any version of Cisco IOS software release 12.0S and later. Non-GSR releases are *not* affected.

The bug ID associated with this error is CSCdm36197.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19990608-ios-grs-acl.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

A GSR running release 11.2(14)GS2 through 11.2(15)GS3 is vulnerable if the keyword **established** is used in an **access-list** statement.

The Cisco 12000 series Gigabit Switch Router is a large rack-mount device, approximately twenty to sixty inches (0.5 to 1.5 meters) tall and twenty inches (0.5 meters) deep, that requires specialized power connections to supply forty to sixty amps of electricity. GSRs are typically used by major Internet Service Providers at their most important interconnection points. If you do not have a Cisco 12000 series GSR, then you are not affected by the vulnerability described in this notice.

Products Confirmed Not Vulnerable

A GSR running release 11.2(15)GS5 and later or any version of release 12.0S is *not* affected.

The Cisco 12000 series Gigabit Switch Router (GSR) is the only Cisco product that is affected by this vulnerability. Currently the 12008 GSR and the 12012 GSR are the only two models in the series.

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

Details

When an affected Cisco Gigabit Switch Router (GSR) executes the following command on an interface:

```
access-list 101 permit tcp any any established
```

the **established** keyword is ignored. This will cause the GSR to forward all TCP traffic for the relevant interface, contrary to the restriction intended in the **access-list** statement.

Impact

This vulnerability can be exploited to circumvent your security policy, resulting in unauthorized access to systems and unauthorized release of information. This may be inadvertent or intentional. Exploiting the flaw requires no special tools or knowledge. It can be determined if your system is vulnerable by attempting to exploit the vulnerability. It is not necessary to make an attempt if it can be determined that you are running one of the affected releases of software on a GSR and a copy of the configuration can be obtained or reverse-engineered.

Software Versions and Fixes

This bug, documented as CSCdm36197, initially appears in 11.2(14)GS2, the first release of Cisco IOS software to support access lists on the GSR.

The bug is present in versions of Cisco IOS software from 11.2(14)GS2 to 11.2(15)GS3, inclusive. The earliest repaired version is 11.2(15)GS5.

If you are running any vulnerable version of 11.2GS and wish to resolve this problem with the least possible change to your existing version of software, you should upgrade to 11.2(15)GS5 or later.

This bug is *not* present in any release of 12.0S, so upgrading to 12.0S or later will also remove the vulnerability.

Workarounds

If you need the functionality provided by the **established** keyword for an **access-list** command, there is no reasonable workaround.

Customers may wish to consider modifying the policies on other network components, if possible, to limit exploitation of this vulnerability until such time as they have downloaded a fixed version of software to the affected GSR.

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 this vulnerability before the date of the public release of this notice. No incidents of malicious exploitation of this vulnerability have been reported to Cisco.

This vulnerability was reported to Cisco by a customer.

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 is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19990608-ios-grs-acl.shtml> on Cisco's Worldwide Web site. In addition to Worldwide Web posting, the initial public version of this notice is being distributed via the following mailing lists and Usenet newsgroups:

- cust-security-announce@cisco.com
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- firewalls@greatcircle.com
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's Worldwide Web server, 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 1.2	1999 June 08	More boilerplate.
Revision 1.1	1999 June 08	Fix boilerplate problems.
Revision 1.0	1999 June 08	Initial public release.

Cisco Security Procedures

Cisco's Worldwide Web site contains complete information for reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information directly from Cisco at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices.

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

Updated: Jun 10, 1999

Document ID: 13656
