

Cisco Security Advisory: Possible Access Control Bypass and Denial of Service in Gigabit Switch Routers Using Gigabit Ethernet or Fast Ethernet Cards

Document ID: 13625

Advisory ID: cisco-sa-20000803-grs-acl-bypass-dos

<http://www.cisco.com/warp/public/707/cisco-sa-20000803-grs-acl-bypass-dos>

Revision 1.0

For Public Release 2000 August 03 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

A defect in Cisco IOS? Software running on all models of Gigabit Switch Routers (GSRs) configured with Gigabit Ethernet or Fast Ethernet cards may cause packets to be forwarded without correctly evaluating configured access control lists (ACLs). In addition to circumventing the access control lists, it is possible to stop an interface from forwarding any packets, thus causing a denial of service.

Only the particular combination of equipment described in this notice is vulnerable. No other combinations of routers and cards are vulnerable.

Network topologies that include a large flat/bridged network may be more susceptible to this vulnerability than some other topologies.

There is no workaround. Customers are urged to upgrade to unaffected versions of software as soon as possible.

This vulnerability is present in all Cisco IOS Software releases for the GSR starting with release 11.2(15)GS1A. Versions of Cisco IOS Software containing the repair for this defect are listed in the section Software Versions and Fixes below.

This defect is documented as Cisco bug ID CSCdp35794.

The complete advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20000803-grs-acl-bypass-dos.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

This vulnerability affects only Gigabit Ethernet and Fast Ethernet cards that are installed in Gigabit Switched Routers.

Products Confirmed Not Vulnerable

Gigabit Switched Routers with other cards are not susceptible to this vulnerability. Similarly, Gigabit Ethernet and Fast Ethernet cards that are installed in other router models are not susceptible to this vulnerability. Specifically, the RSP/7200 series routers are *not* affected.

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

Details

When access lists are used on a GSR with Gigabit Ethernet or Fast Ethernet cards installed and configured, line card failures may occur that require a reset of the affected card and internal queuing data structures may be corrupted. The problem is due to differences in the optimized handling of certain types of packets from shared media that directly affects the evaluation of access control lists on Gigabit Ethernet and Fast Ethernet interfaces. The problem is more likely to occur on a large shared or bridged Ethernet segment, and is more evident with the use of compiled access control lists (also known as Turbo ACLs) than with other access control lists. The problem cannot occur unless access control lists are configured on the affected interfaces.

This defect has been assigned Cisco bug ID CSCdp35794. If you are a registered CCO user and you have logged in, you can view bug details.

Impact

Under certain conditions it is possible to circumvent compiled access control lists with a moderate probability of success and circumvent extended access control lists with a low probability of success. A possible side effect is that the attacked interface may stop forwarding packets without logging an error, requiring the card to be reset via software.

Due to the nature of this vulnerability, it is difficult to predict the exact results of any such exploitation.

Network topologies that include a large flat/bridged network (several hundred hosts or more) may be more susceptible to this vulnerability than some other topologies. However, by sending a large number of specific

packets, it may be possible to trigger this vulnerability on any topology.

Software Versions and Fixes

This vulnerability affects Gigabit Ethernet and Fast Ethernet cards on the following Gigabit Switch Routers:

- 12008 Gigabit Switch Router
- 12012 Gigabit Switch Router
- 12016 Gigabit Switch Router

This vulnerability affects all releases of Cisco GSR IOS Software starting with 11.2(15)GS1A. This vulnerability has been corrected in the following IOS releases:

- 11.2(19)GS0.2
- 12.0(8.0.2)S
- 12.0(7)S1
- 12.0(7.4)S
- 12.0(8.3)SC
- 12.0(7)SC

All subsequent releases of Cisco IOS Software for the GSR incorporate this fix.

To determine if your system is affected by this problem, execute the **show version** command while in global configuration mode. If the output does not contain the words "GS Software" in the banner and "FastEthernet" or "GigabitEthernet" in the list of installed cards, then the system is not affected by the vulnerability described in this advisory.

If **show version** displays "GS Software" and also reports that "FastEthernet" or "GigabitEthernet" cards are installed in the system, then the current IOS release number should be compared to those listed above to determine if an upgrade is necessary.

Workarounds

There is no known configuration workaround. Customers are urged to upgrade affected platforms to a fixed software version as soon as possible.

Affected line cards that have stopped forwarding packets can be reset by using the command **microcode reload [optional-slot-number]** while in global configuration mode.

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.

Cisco Security Advisory: Possible Access Control Bypass and Denial of Service in Gigabit Switch Routers U

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

The Cisco PSIRT has received no reports of malicious exploitation of this vulnerability.

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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20000803-grs-acl-bypass-dos.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 (includes CERT/CC)
- bugtraq@securityfocus.com
- firewalls@lists.gnac.com
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- Various internal Cisco mailing lists

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	2000 August 03	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>.

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

Updated: Aug 03, 2000

Document ID: 13625
