

# Multiple Vulnerabilities in Access Control List Implementation for Cisco 12000 Series Internet Router

Advisory ID: [cisco-sa-20011114-gsr-acl](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20011114-gsr-acl.shtml>

## Revision 1.1

Last Update 2001 November 15 0800 UTC (GMT)

For Public Release 2001 November 14 1600 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

## Contents

- [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

Six vulnerabilities involving Access Control List (ACL) has been discovered in multiple releases of Cisco IOS® Software Release for Cisco 12000 Series Internet Routers. Not all vulnerabilities are present in all IOS releases and only line cards based on the Engine 2 are affected by them.

No other Cisco product is vulnerable.

The workarounds are described in the Workarounds section.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20011114-gsr-acl.shtml>

## ☐ Affected Products

This section provides details on affected products.

### ☐ Vulnerable Products

Only Cisco 12000 Series Internet Routers with line cards based on Engine 2 are affected with these vulnerabilities. Not all line cards of a Cisco 12000 Series are affected by all vulnerabilities. Vulnerabilities are present in the underlying technology an individual line card is based upon. That technology is called "Engine". Currently Cisco is shipping line cards based on the following Engines: 0, 1, 2, 3 and 4.

To determine what Engine your card is based on, you need to log on the Cisco 12000 router and issue "**sh diag**" command while in enable mode. The engine type will be displayed as "**L3 Engine: x**" where **x** will be the corresponding number.

The following example shows the output for an Engine 2 based line card.

```
c12000#sh diag
SLOT 1 (RP/LC 1 ): 1 Port Packet Over SONET OC-48c/STM-16 Single Mode/SR SC-SC
connector

MAIN: type 41, 800-5271-01 rev A0 dev 0

HW config: 0x04 SW key: 00-00-00

PCA: 73-3295-05 rev A0 ver 5

HW version 1.1 S/N SDK034004AY

MBUS: Embedded Agent

Test hist: 0x00 RMA#: 00-00-00 RMA hist: 0x00

DIAG: Test count: 0x00000000 Test results: 0x00000000
L3 Engine: 2 - Backbone OC48 (2.5 Gbps)

^^^^^^^^^^^^ <- Note the engine type

[further output truncated]
```

These vulnerabilities are affecting line cards based on Engine 2.

### ☐ Products Confirmed Not Vulnerable

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

## ☐ Details

Six vulnerabilities were found in IOS releases that are supporting Cisco 12000 platforms. Only line cards based on Engine 2 are affected.

- **CSCdm44976**

ACL will not block non initial fragments of a packet. This Cisco bug ID is adding a support for "**fragment**" keyword in the ACL. The White Paper [Access Control Lists and IP Fragments](#) describes how keyword

fragment modifies behavior of ACL.

- **CSCdu57417**  
The keyword "**fragment**" in the compiled ACL (Turbo ACL) is ignored if a packet is destined to the router itself.
- **CSCdu03323**  
The implicit "**deny ip any any**" rule at the end of an ACL is ignored if an ACL of exactly 448 entries is applied on an interface as an outgoing ACL. An ACL with any other number of rules, greater or less than 448, is unaffected by this vulnerability.
- **CSCdu35175**  
A support for "**fragment**" keyword in an outgoing ACL is added. Previously, only incoming ACL supported this keyword and outgoing ACL was ignoring it.
- **CSCdt96370**  
An outbound Access Control List (ACL) may not block all intended traffic on a router when an input ACL is configured on some, but not all, interfaces of a multi port Engine 2 line card. The prerequisite is that, the traffic in question, was not filtered by an inbound ACL on the ingress port. An ACL applied at the ingress point will work as expected and block desired traffic.
- **CSCdt69741**  
Packet fragments are not filtered by the ACL despite using "**fragment**" keyword. The White Paper [Access Control Lists and IP Fragments](#) describes how keyword fragment modifies behavior of ACL.

[Top of the section](#)   [Close Section](#)

## ☐ Impact

Successful exploitation of these vulnerabilities may result in these issues:

- **CSCdm44976**  
The router will not block all traffic. By sending an offending traffic in packet fragments it is possible to circumvent the protection offered by ACL and cause Denial-of-Service for the protected IP address.
- **CSCdu57417**  
It is possible to cause the Denial-of-Service on the router itself if sufficient amount of traffic is sent to the router. This offending traffic should be send as packet fragments.
- **CSCdu03323**  
If an outgoing ACL contains exactly 448 entries and if explicit rule "**deny ip any any**" is not present as the last statement, the ACL will fail to drop packets. Our tests shows that only 50% of packets are dropped. This may allow some undesired traffic to pass into the protected network thus violating security policy.
- **CSCdu35175**  
Fragmented packets may be allowed into the protected network if the keyword "**fragment**" was applied to an outgoing ACL.
- **CSCdt96370**  
This vulnerability can cause unwanted traffic to be allowed in and out of the protected network. The security based on an ACL will be breached completely.
- **CSCdt69741**  
This vulnerability can be exploited to attack systems that are supposed to be protected by the ACL on the router.

[Top of the section](#)   [Close Section](#)

## ☐ Software Versions and Fixes

Each row of the table describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix and the anticipated date of availability for each are listed in the "Rebuild", "Interim", and "Maintenance" columns. A device running any

release in the given train that is earlier than the release in a specific column (less than the earliest fixed release) is known to be vulnerable, and it should be upgraded at least to the indicated release or a later version (greater than the earliest fixed release label).

When selecting a release, keep in mind the following definitions:

### Maintenance

Most heavily tested and highly recommended release of any label in a given row of the table.

### Rebuild

Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific defect. Although it receives less testing, it contains only the minimal changes necessary to effect the repair.

### Interim

Built at regular intervals between maintenance releases and receives less testing. Interim releases should be selected only if there is no other suitable release that addresses the vulnerability, and interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available via manufacturing, and usually they are not available for customer download from CCO without prior arrangement with the Cisco TAC.

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 TAC for assistance as shown in the following section.

More information on Cisco IOS software release names and abbreviations is available at <http://www.cisco.com/web/about/security/intelligence/ios-ref.html>.

Train	Description of Image or Platform	Availability of Fixed Releases*		
Vulnerability CSCdm4476		Rebuild	Interim**	Maintenance
12.0S	Core/ISP support: GSR, RSP, c7200		12.0(10.1)S	12.0(11)S
Vulnerability CSCdu57417		Rebuild	Interim**	Maintenance
12.0S	Core/ISP support: GSR, RSP, c7200		12.0(19.3)S	12.0(19)S

12.0ST	Early deployment (ED) release for the Cisco 7200, 7500/7000RSP and 12000 series routers for Service Providers (ISPs).	12.0(18.6)ST1	12.0(19.3)ST	12.0(19)ST
Vulnerability CSCdu03323		Rebuild	Interim**	Maintenance
12.0S	Core/ISP support: GSR, RSP, c7200	12.0(16)S2	12.0(17.5)S	12.0(17)S
12.0ST	Early deployment (ED) release for the Cisco 7200, 7500/7000RSP and 12000 series routers for Service Providers (ISPs).	12.0(16.6)ST1	12.0(17.5)ST	12.0(17)ST
Vulnerability CSCdu35175		Rebuild	Interim**	Maintenance
12.0S	Core/ISP support: GSR, RSP, c7200		12.0(19.6)S	
12.0ST	Early deployment (ED) release for the Cisco 7200, 7500/7000RSP and 12000 series routers		12.0(19.6)ST	

	for Service Providers (ISPs).			
Vulnerability CSCdt96370		Rebuild	Interim**	Maintenance
12.0S	Core/ISP support: GSR, RSP, c7200	12.0(16)S1	12.0(17.1)S	12.0(17)S
12.0ST	Cisco IOS software Release 12.0ST is an early deployment (ED) release for the Cisco 7200, 7500/7000RSP and 12000 (GSR) series routers for Service Providers (ISPs).	12.0(15.6)ST3	12.0(17.1)ST	12.0(16)ST
Vulnerability CSCdt69741		Rebuild	Interim**	Maintenance
12.0S	Core/ISP support: GSR, RSP, c7200	12.0(16.6)S2	12.0(17.3)S	12.0(17)S
12.0ST	Cisco IOS software Release 12.0ST is an early deployment (ED) release for the Cisco 7200, 7500/7000RSP and 12000		12.0(17.3)ST	12.0(18)ST

(GSR) series routers for Service Providers (ISPs).			
Notes			
* All dates are estimates and subject to change. ** Interim releases are subjected to less rigorous testing than regular maintenance releases, and may have serious bugs.			

[Top of the section](#)   [Close Section](#)

## ☐ Workarounds

### **CSCddm44976**

There is no direct workaround for this vulnerability. If feasible, packet fragments may be filtered before they reach the GSR.

### **CSCdu57417**

There is no direct workaround for this vulnerability. If feasible, packet fragments may be filtered before they reach the GSR.

### **CSCdu03323**

The workaround is to either shorten the ACL to be less than 448 lines in length or to explicitly add rule "**deny ip any any**" as the last statement.

### **CSCdu35175**

The workaround is to transform an ACL to an incoming ACL instead of the outgoing one.

### **CSCdt96370**

Apply an ACL on all ports on the ingress line card. If a particular port is supposed to not block any traffic, then apply the ACL of the form `access-list xy permit ip any any`.

### **CSCdt69741**

There is no direct workaround for this vulnerability. It is possible to block the fragments on an intermediate router, if such exists, that should be placed between the affected Cisco 12000 and the final target. The intermediate router must not be another Cisco 12000 affected by the same vulnerability.

[Top of the section](#)   [Close Section](#)

## ☐ 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.

[Top of the section](#)   [Close Section](#)

## ☐ **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>.

[Top of the section](#)   [Close Section](#)

## ☐ **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.

[Top of the section](#)   [Close Section](#)

## ☐ **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](mailto: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.

[Top of the section](#)   [Close Section](#)

## ☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

[Top of the section](#)   [Close Section](#)

## ☐ **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.

[Top of the section](#)   [Close Section](#)

## ☐ **Distribution**

This notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20011114-gsr-acl.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](mailto:cust-security-announce@cisco.com)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [firewalls@lists.gnac.com](mailto:firewalls@lists.gnac.com)
- Various internal Cisco mailing lists

Future updates of this notice, 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 URL given above for any updates.

[Top of the section](#)   [Close Section](#)

## ☐ **Revision History**

Revision 1.1	2001-November-15	Update table with fixed IOS releases
Revision 1.0	2001-November-14	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 Web site at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](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>

### Help us help you.

#### Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

#### This document solved my problem.

- Yes
- No
- Just browsing

#### Suggestions for improvement:

(256 character limit)

