

Cisco Security Advisory: ICMP Unreachable Vulnerability in Cisco 12000 Series Internet Router

Document ID: 17590

Advisory ID: cisco-sa-20011114-gsr-unreachable

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

Revision 1.2

Last Updated 2006 November 07 0100 UTC (GMT)

For Public Release 2001 November 14 1600 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 performance of Cisco 12000 series routers can be degraded when they have to send a large number of ICMP unreachable packets. This situation usually can occur during heavy network scanning. This vulnerability is tracked by three different bug IDs: [CSCdr46528](#) ([registered](#) customers only) , [CSCdt66560](#) ([registered](#) customers only) , and [CSCds36541](#) ([registered](#) customers only) . Each bug ID is assigned to a different Engine the line card is based upon.

The rest of the Cisco routers and switches are not affected by this vulnerability. It is specific for Cisco 12000 Series.

No other Cisco product is vulnerable.

The workaround is to either prevent the router from sending unreachable Internet Control Message Protocol (ICMPs) at all or to rate limit them.

This advisory is available at

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

Affected Products

This section provides details on affected products.

Vulnerable Products

Only Cisco 12000 Series Internet Routers are affected with this vulnerability. No other routers or switches are affected. Not all line cards of the Cisco 12000 Series are affected by this vulnerability. Vulnerability is 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 the **show 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#show 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]
```

All line cards that are based on the Engines 0, 1 and 2 are vulnerable. Line cards based on the Engine 3 and 4 are not affected.

The following table depicts which Cisco IOS® Software Release is vulnerable to a particular issue:

DDTS	12.0S	12.0ST
CSCdr46528 (registered customers only)	Vulnerable	Vulnerable
CSCds36541 (registered customers only)	Vulnerable	Vulnerable
CSCdt66560 (registered customers only)	Vulnerable	Vulnerable

Products Confirmed Not Vulnerable

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

Details

The received packet will be dropped when either there is no valid path to the destination or when the packet should be routed to the Null0 interface. The packets are either fast dropped (Engine 0 Line Cards) or hardware dropped (all other application-specific integrated circuit (ASIC) based forwarding Line Cards). Given the fast and hardware drop capabilities of the Cisco 12000, a large volume of traffic can be dropped without impacting the capabilities of the router. Whenever a packet is dropped the router must send an ICMP unreachable packet

back to the source. That is mandated by the Internet Standards.

When a high volume of traffic is sent to the router that requires ICMP unreachable replies, the processing of the replies can saturate the CPU. This condition can happen when the router is "Black Hole" filtering, dropping packets sent to it as the network's default path, or from a direct Denial of Service (DOS) against the router. For further information on "Black Hole" filtering, refer to [Essential IOS Features Every ISP Should Consider](#), section "Black Hole Routing as a Packet Filter".

The following table shows the relationship between the vulnerabilities and Engine the line card is based on.

DDTS	Engine 0	Engine 0	Engine 2	Engine 4
CSCdr46528	Vulnerable			
CSCds36541		Vulnerable		
CSCdt66560			Vulnerable	

Impact

Exploitation of these vulnerabilities may lead to the Denial-of-Service. The router's performance will degrade and, in the worst case scenario, the router will stop forwarding packets.

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.

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 contains 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.

More information on Cisco IOS software release names and abbreviations is available at <http://www.cisco.com/warp/public/620/1.html>.

Train	Description of Image or Platform	Availability of Fixed Releases*		
		Rebuild	Interim**	Maintenance
Vulnerability CSCdr46528				
12.0S	Core/ISP support: GSR, RSP, c7200	12.0(16)S1	12.0(16.5)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(16.5)ST	12.0(16)ST
Vulnerability CSCds36541				
12.0S	Core/ISP support: GSR, RSP, c7200	12.0(13.6)S2	12.0(14.1)S	12.0(14)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		12.0(14.3)ST	

	Service Providers (ISPs).			
Vulnerability CSCdt66560		Rebuild	Interim**	Maintenance
12.0S	Core/ISP support: GSR, RSP, c7200	12.0(16)S1	12.0(16.6)S	12.0(17)S
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.				

Workarounds

There are two workarounds for this issue. The first one is to prevent the router from sending ICMP unreachables at all. That behavior is governed with the **no ip unreachable** command. This command should be applied on an interface, such as in this example:

```
router(config)#interface ethernet 0
router(config-if)#no ip unreachable
```

It is possible to mitigate the problem by rate limiting number of ICMP unreachable packets that are sent. Here is the example:

```
router(config)#ip icmp rate-limit unreachable n
```

Where **n** is the number of milliseconds between two consecutive ICMP unreachable packets. The default value is 500. That means that one ICMP unreachable packet is send every 500 ms.

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

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

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-20011114-gsr-unreachable.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 1.2	2006-Nov-06	Fixed URL to Black Hole filtering.
Revision 1.1	2001-Nov-15	Changed tables entries for the Affected Products and Software Versions and Fixes sections.
Revision 1.0	2001-Nov-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 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](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Nov 07, 2006

Document ID: 17590
