

Cisco Security Advisory: Data Leak with Cisco Express Forwarding Enabled

Document ID: 20640

Advisory ID: cisco-sa-20020227-ios-cef

<http://www.cisco.com/warp/public/707/cisco-sa-20020227-ios-cef.shtml>

Revision 1.3

Last Updated 2002 April 11 1400 UTC (GMT)

For Public Release 2002 February 27 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: **INTERIM**
- Distribution
- Revision History
- Cisco Security Procedures

Summary

Excluding Cisco 12000 Series Internet Routers, all Cisco devices running Cisco IOS® software that have Cisco Express Forwarding (CEF) enabled can leak information from previous packets that have been handled by the device. This can happen if the packet length described in the IP header is bigger than the physical packet size. Packets like these will be expanded to fit the IP length and, during that expansion, an information leak may occur. Please note that an attacker can only collect parts of some packets but not the whole session.

No other Cisco product is vulnerable. Devices that have fast switching enabled are not affected by this vulnerability. Cisco 12000 Series Internet Routers are not affected by this vulnerability.

The workaround for this vulnerability is to disable CEF.

This advisory is available at the <http://www.cisco.com/warp/public/707/cisco-sa-20020227-ios-cef.shtml>.

Affected Products

Vulnerable Products

All Cisco IOS releases that are supporting CEF are vulnerable. In order to trigger this vulnerability CEF must be enabled on the device. The vulnerable Cisco IOS releases are (this is not an exhaustive list):

- 11.1CC
- 12.0, 12.0S, 12.0T, 12.0ST
- 12.1, 12.1E, 12.1T
- 12.2, 12.2T

Products Confirmed Not Vulnerable

No other Cisco products are affected. Specifically, the following products are not vulnerable:

- Cisco 12000 Series Internet Routers
- Catalyst 6000 with both Supervisor Engine I and II

Details

When a router receives a packet where MAC level packet length is shorter than is indicated by the IP level, the router will "extend" the packet to the size indicated by the IP level. This extension will be done by padding the packet with an arbitrary data. The issue here is that padding may contain data from a previous packet that has not been erased.

Although it is possible to trigger this vulnerability on command, it is not possible to predict what information would be collected this way. It is not possible for an attacker to selectively capture desired packets (for example, packets with username and password combination).

This vulnerability is specific to CEF. Fast switching is not affected by it.

This vulnerability is documented as Cisco Bug ID CSCdu20643. For the Cisco IOS 11.1CC image, this vulnerability is described as Cisco Bug ID CSCdp58360.

Impact

By sending malformed packets, and capturing them after they have been processed by CEF, an attacker may find remnants of previous packets in them. The remnant data may contain whatever the previous packet has carried. That may be parts of a document, mail or any other content.

Note: In an interactive session such as typing a password, characters are sent one by one in separate packets. That drastically lowers the probability that all packets will be captured. In addition, it is almost certain that typed characters will be overwritten by the contents of the attacking packets.

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

Cisco Security Advisory: Data Leak with Cisco Express Forwarding Enabled

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. Interims 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 Technical Assistance Center (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/warp/public/620/1.html>.

Train	Description of Image or Platform	Availability of Fixed Releases*		
11.1–based Releases		Rebuild	Interim**	Maintenance
11.1CC	ED release for 7000 series	11.1(36)CC3		
12.0–based Releases		Rebuild	Interim**	Maintenance
12.0	GD release for all platforms		12.0(20.4)	
12.0S	ED release for all platforms	12.0(17)ST4	12.0(18.3)S	12.0(19)S
12.0ST	ED release for all platforms		12.0(18.3)ST	12.0(19)ST
12.0T	ED release for all platforms	To be decided		
12.0W5			12.0(20.4)W5(24.7)	

	ED release for all platforms			
12.1–based Releases		Rebuild	Interim**	Maintenance
12.1	LD release for all platforms		12.1(9.2)	12.1(10)
12/1E	ED release for all platforms	12.1(8.5)E2	12.1(9.5)E	12.1(8a)E
12.1EC	ED release for all platforms	12.1(7.5)EC1	12.1(9.5)EC	
12.1T	ED release for all platforms	To be decided		
12.1XM	ED release for all platforms	12.1(5) XM6		
12.2–based Releases		Rebuild	Interim**	Maintenance
12.2	LD release for all platforms		12.2(2.5)	12.2(3)
12.2S	LD release for all platforms		12.2(3.3)S	
12.2T	ED release for all platforms		12.2(2.4)T	12.2(4)T

Workarounds

The workaround is to disable CEF on a router.

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 vulnerabilities described in this advisory.

Status of This Notice: INTERIM

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. CISCO EXPECTS TO UPDATE

THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

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 will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20020227-ios-cef.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
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- 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.

Revision History

Revision 1.3	2002-April-11	Added Catalyst 6000 with both Supervisor Engine I and II to products not affected in Affected Products section
Revision 1.2	2002-February-28	Removed reference to dCEF in Affected Products section
Revision 1.1	2002-February-28	Added Cisco 12000 Series Internet Routers to products not affected
Revision 1.0	2002-February-27	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.

Cisco Security Advisory: Data Leak with Cisco Express Forwarding Enabled

