

Cisco Security Advisory: A Vulnerability in IOS Firewall Feature Set

Document ID: 9360

Advisory ID: cisco-sa-20011128-ios-cbac-dynacl

<http://www.cisco.com/warp/public/707/cisco-sa-20011128-ios-cbac-dynacl.shtml>

Revision 1.3

Last Updated 2006 July 13 1800 UTC (GMT)

For Public Release 2001 November 28 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 IOS Firewall Feature set, also known as Cisco Secure Integrated Software, also known as Context Based Access Control (CBAC), and introduced in IOS version 11.2P, has a vulnerability that permits traffic normally expected to be denied by the dynamic access control lists.

This vulnerability is documented as Cisco Bug ID CSCdv48261.

No other Cisco product is vulnerable.

There is no workaround.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20011128-ios-cbac-dynacl.shtml>

Affected Products

This section provides details on affected products.

Vulnerable Products

Only configurations implementing CBAC are affected. An affected configuration includes the lines "ip inspect" in your router's configuration. Here is one example:

```
ip inspect name rule1 udp
ip inspect name rule1 tcp
!
!
interface FastEthernet0/1
ip address 1.2.3.4 255.255.255.0
ip inspect rule1 in
duplex auto
speed auto
!
```

The filename of the router image, available via **show version** command, includes an "o" in the section between the hyphens, if the software includes the IOS Firewall Featureset, as in the following example.

```
Router>show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IO3-M),
Version 12.1(5)T, RELEASE SOFTWARE (fc1)
(the rest is truncated)
```

In this example the image file name is c2600-io3-m. Since it has an "o" in its name, this image can support CBAC. For additional information regarding Cisco IOS image identifiers consult the document at <http://www.cisco.com/warp/public/620/1.html#t16>. The major affected Cisco IOS trains are:

- 11.2P
- 11.3T
- 12.0, 12.0T
- 12.1, 12.1T, 12.1E
- 12.2, 12.2T

In addition to these, several Early Deployment (also known as X releases) are affected. The complete list is given in the Software Versions and Fixes section of this advisory.

Affected hardware models are:

- Cisco routers in the following series: 800, 820, 950, 1400, 1600, 1700, 2500, 2600, 3600, 4000 Gateway, 4224, 7100, 7200, 7400, 7500, SOHO 70, ubr900, ICS7750.
- The Catalyst 5000 and 6000 if they are running Cisco IOS software.

Products Confirmed Not Vulnerable

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

Details

Cisco IOS Firewall is a packet inspection system. It is also a stateful system; it keeps information about connections that last beyond the lifetime of a single packet. CBAC is an IP-only feature. A router running CBAC recognizes Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and some higher-layer protocols, and examines packet data beyond the IP headers. If configured, CBAC maintains session information based on packets examined.

When a session is initiated from the protected network, CBAC creates a dynamic access list entry allowing return traffic for that session. Upon inspection of the return traffic through a dynamic access list, source and destination addresses and ports are checked, however IP protocol type is not checked. This could allow a packet of different protocol type into the protected network.

This vulnerability is documented as Cisco Bug ID **CSCdv48261**.

Impact

By allowing packets of different type into the protected network, the customer is exposed to much bigger threat. This vulnerability can be exploited for reconnaissance purposes, but only for a single port and host that initiated a session in the first place. Depending on the exact session parameters, it may be possible to send data to processes that were supposed to be accessible only from within the trusted network. In the worst case, it is possible to open an interactive session to a host on the protected network. In that case, there must be a process running on the host that is listening to the port for which a hole is opened by CBAC.

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 a 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. The release 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. 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 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.x-based Releases		Rebuild	Interim**	Maintenance
11.2P	Early Deployment: limited	End of Support Upgrade recommended to 12.0		

	platforms			
11.3T		End of Support Upgrade recommended to 12.0		
12.0-based Releases		Rebuild	Interim**	Maintenance
12.0	General deployment release for all platforms		12.0(20.3) Available 2001–November–26	12.0(21) Available 2002–January–07
12.0T	Early Deployment: various platforms	Not scheduled Upgrade recommended to 12.1		
12.0XA	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.1		
12.0XB	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.1		
12.0XC	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.1		
12.0XD	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.1		
12.0XE	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.1		
12.0XG	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.1		
12.0XI	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.1		
12.0XK	Early Deployment	End of Engineering Upgrade recommended to 12.1		

	(ED) for selected platforms			
12.0XM	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.1		
12.0XQ	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.1		
12.0XR	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.1		
12.0XV	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.1		
12.1–based Releases		Rebuild	Interim**	Maintenance
12.1	Limited deployment release for all platforms	12.1(11a)	12.1(11.1)	12.1(12) Available 2001–December–03
12.1E	Core/ISP support: GSR, RSP, c7200		12.1(9.6)E	12.1(10)E
12.1E	Catalyst 6000	12.1(8a)E5		
12.1T	Early Deployment (ED): VPN, Distributed Director, various platforms	End of Engineering Upgrade recommended to 12.2		
12.1XB	Early Deployment (ED) for selected platforms	Not scheduled Upgrade recommended to 12.1(5)YB1		
12.1XC	Early Deployment (ED) for	End of Engineering Upgrade recommended to 12.2		

	selected platforms			
12.1XF	Early Deployment (ED) for selected platforms	12.1(2)XF5 Available 2002–January		
12.1XG	Early Deployment (ED) for selected platforms	12.1(3)XG6 Available 2002–January		
12.1XH	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.2		
12.1XI	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.2		
12.1XJ	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.1(5)YB		
12.1XK	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.2		
12.1XL	Early Deployment (ED) for selected platforms	End of Engineering Upgrade recommended to 12.2		
12.1XM	Early Deployment (ED) for selected platforms	12.1(5)XM6 Available 2001–December–03		
12.1XP	Early Deployment (ED) for selected platforms	Not scheduled Migration recommended to 12.2T		
12.1XT	Early Deployment	Not scheduled Migration recommended to 12.2T		

	(ED) for selected platforms			
12.1YB	Early Deployment (ED) for selected platforms	12.1(5)YB5 Available 2002–January		
12.1YC	Early Deployment (ED) for selected platforms	12.1(5)YC2 Available 2002–January		
12.1YE	Early Deployment (ED) for selected platforms	12.1(5)YE4		
12.1YF	Early Deployment (ED) for selected platforms	12.1(5)YF3 Available 2001–November		
12.2–based Releases		Rebuild	Interim**	Maintenance
12.2	Limited deployment release for various platforms		12.2(5.7)	12.2(6) Available 2001–November–12
12.2DD	Early Deployment (ED) for selected platforms	Not scheduled Upgrade recommended to 12.2(4)B		
12.2T	Early deployment release for various platforms		12.2(5.7)T	12.2(8)T Available 2002–February–28
12.2XD	Early Deployment (ED) for selected platforms	12.2(2)XD3 Available 2002–January		
12.2XE	Early Deployment (ED) for selected platforms	12.2(1)XE2 Available 2002–January		

12.2XH	Early Deployment (ED) for selected platforms	12.2(2)XH2 Available 2002 –January		
12.2XI	Early Deployment (ED) for selected platforms	12.2(2)XI1 Available 2002 –January		
12.2XJ	Early Deployment (ED) for selected platforms	12.2(2)XJ1 Available 2002 –January		
12.2XK	Early Deployment (ED) for selected platforms	12.2(2)XK5 Available 2002 –January		
12.2XQ	Early Deployment (ED) for selected platforms	12.2(2)XQ2 Available 2002 –January		

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 is no workaround.

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

This vulnerability was discovered by a customer. The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities 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 notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20011128-ios-cbac-dynacl.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 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 1.3	2006-July-13	Fixed software table for 12.2 based releases.
Revision 1.2	2002-January-02	In the software information table on release 12.2T, added the release date as February 28, 2002. Also changed the next release version to 12.2(8)T. Deleted the rebuild version because there is no rebuild.
Revision 1.1	2001-November-29	In the table with fixed releases, in the row for 12.2T, added a T to the maintenance release 12.2(7)T.
Revision 1.0	2001-November-28	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>.

