

Cisco Security Advisory: Cisco IOS Software Input Access List Leakage with NAT

Document ID: 13659

Advisory ID: cisco-sa-19990414-ios-nat-acl

<http://www.cisco.com/warp/public/707/cisco-sa-19990414-ios-nat-acl.shtml>

Revision 1.3

For Public Release 1999 April 14 1800 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 group of related software bugs (bug IDs given under "Software Versions and Fixes") create an undesired interaction between network address translation (NAT) and input access list processing in certain Cisco routers running 12.0-based versions of Cisco IOS software (including 12.0, 12.0S, and 12.0T, in all versions up to, but not including, 12.0(4), 12(4)S, and 12.0(4)T, as well as other 12.0 releases). Non-12.0 releases are not affected.

This may cause input access list filters to "leak" packets in certain NAT configurations, creating a security exposure. Configurations without NAT are not affected.

The failure does not happen at all times, and is less likely under laboratory conditions than in installed networks. This may cause administrators to believe that filtering is working when it is not.

Software fixes are being created for this vulnerability, but are not yet available for all software versions (see the section on "Software Versions and Fixes"). This notice is being released before fixed software is universally available in order to enable affected Cisco customers to take immediate steps to protect themselves against this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19990414-ios-nat-acl.shtml>.

Cisco Security Advisory: Cisco IOS Software Input Access List Leakage with NAT

Affected Products

This section provides details on affected products.

Vulnerable Products

If you are using input access lists in conjunction with NAT on an interface of a Cisco IOS router running any 12.0-based version of Cisco IOS software earlier than the fixed versions listed in the table under "Software Versions and Fixes", then you are affected by this vulnerability. Non-12.0 releases are *not* affected.

Both input access lists and NAT must be in use on the same router interface in order for this vulnerability to manifest itself. If your configuration file does not contain the command `ip access-group <acl> in` on the same interface with `ip nat inside` or `ip nat outside`, then you are *not* affected. The majority of routers are not configured to use NAT, and are therefore *not* affected. NAT routers are most commonly found at Internet boundaries.

Cisco devices that run Cisco IOS software, and are affected by this vulnerability, include the following:

- Cisco routers in the 17xx family are affected.
- Cisco routers in the 26xx family are affected.
- Cisco routers in the 36xx family are affected.
- Cisco routers in the AS58xx family (not the AS52xx or AS53xx) are affected.
- Cisco routers in the 72xx family (including theubr72xx) are affected.
- Cisco routers in the RSP70xx family (not non-RSP 70xx routers) are affected.
- Cisco routers in the 75xx family are affected.
- The Catalyst 5xxx Route-Switch Module (RSM) is affected. The Catalyst 5xxx switch supervisors themselves are not affected; only the optional RSM module is involved.

Cisco devices which run Cisco IOS software, but are *not* affected by this vulnerability, include the following:

- Cisco routers in the 8xx family are *not* affected.
- Cisco routers in theubr9xx family are *not* affected.
- Cisco routers in the 10xx family are *not* affected.
- Cisco routers in the 14xx family are *not* affected.
- Cisco routers in the 16xx family are *not* affected.
- Cisco routers in the 25xx family are *not* affected.
- Cisco routers in the 30xx family are *not* affected (and do not run 12.0 software).
- Cisco routers in the mc38xx family are *not* affected.
- Cisco routers in the 40xx family are *not* affected.
- Cisco routers in the 45xx family are *not* affected.
- Cisco routers in the 47xx family are *not* affected.
- Cisco routers in the AS52xx family are *not* affected.
- Cisco routers in the AS53xx family are *not* affected.
- Catalyst 85xx Switch Routers are *not* affected (and do not support NAT).
- GSR12xxx Gigabit Switch Routers are *not* affected (and do not support NAT).
- Cisco 64xx universal access concentrators are *not* affected.
- Cisco AGS/MGS/CGS/AGS+ and IGS routers are *not* affected (and do not run 12.0 software).
- LS1010 ATM switches are *not* affected.
- Catalyst 2900XL LAN switches are *not* affected.
- The Cisco DistributedDirector is *not* affected.

If you are unsure whether your device is running classic Cisco IOS software, log into the device and issue the command **show version**. Cisco IOS software will identify itself simply as "IOS" or "Internetwork Operating System Software". Other Cisco devices either will not have the **show version** command, or will give different output.

Products Confirmed Not Vulnerable

If you are not running Cisco IOS software, then you are *not* affected by this vulnerability. Cisco devices which do *not* run Cisco IOS software, and are *not* affected by this vulnerability, include the following:

- 7xx dialup routers (750, 760, and 770 series) are *not* affected.
- Catalyst 19xx, 28xx, 29xx, 3xxx, and 5xxx LAN switches are *not* affected.
- WAN switching products in the IGX and BPX lines are *not* affected.
- The MGX (formerly known as the AXIS shelf) is *not* affected.
- *No* host-based software is affected.
- The Cisco PIX Firewall is *not* affected.
- The Cisco LocalDirector is *not* affected.
- The Cisco Cache Engine is *not* affected.

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

Details

This vulnerability is created by bugs in interface hardware drivers. These bugs affect the drivers for all interface types on affected platforms. The majority of these driver bugs are grouped under Cisco bug ID CSCdk79747. Additional bugs IDs include CSCdm22569 (miscellaneous additional drivers), and CSCdm22299 (Cisco 1400 and 1700 platforms; of these two, only the 1700 actually suffers packet leakage).

A related bug is CSCdm22451, which describes a problem with the original fix for CSCdk79747.

All four of these bugs are, or will be, fixed in the software releases listed in the table below.

Impact

The severity of the impact may vary, depending on the device type, configuration and environment, from sporadic leakage of occasional packets to consistent leakage of significant classes of packets. The environment dependencies are extremely complex and difficult to characterize, but essentially all vulnerable configurations are affected to some degree. Customers with affected devices are advised to assume that the vulnerability affects their networks whenever input access lists are used together with NAT in 12.0-based software.

This vulnerability may allow users to circumvent network security filters, and therefore security policies. This may happen with no special effort on the part of the user, and indeed without the user being aware that a filter exists at all. No particular tools, skills, or knowledge are needed for such opportunistic attacks. In some configurations, it may be also possible for an attacker to deliberately create the conditions for this failure; doing this would require detailed knowledge and a degree of sophistication.

The conditions that trigger this vulnerability may be frequent and long-lasting in some production configurations.

Software Versions and Fixes

Many Cisco software images have been or will be specially reissued to correct this vulnerability. For example, regular released version 12.0(3) is vulnerable, as are interim versions 12.0(3.1) through 12.0(3.7). The first fixed version of 12.0 mainline software is 12.0(4). However, a special release, 12.0(3b), contains only the security vulnerability fixes, and does not include any of the other bug fixes from later 12.0 interim releases.

If you were running 12.0(3), and wanted to upgrade to fix this problem, without taking the risk of instability presented by the new functionality and additional bug fixes in the 12.0(4) release, you could upgrade to 12.0(3b). 12.0(3b) represents a "code branch" from the 12.0(3) base, which merges back into the 12.0 mainline at 12.0(4).

In every case, these special releases are one-time spot fixes, and will not be maintained. The upgrade path from, say, 12.0(3b), is to 12.0(4).

Note that fixes are not yet available for some affected releases. Cisco is releasing this notice before the general release of fixed software because of the possibility that this vulnerability may be exploited in the interim. All fix dates in the table are estimates and are subject to change.

Cisco IOS Major Release	Description	Special spot fix release; most stable immediate upgrade path (see above)	Projected first fixed regular or interim** release (fix will carry forward into all later versions)	Projected first fixed regular maintenance release (or other long term upgrade path)
Unaffected releases				
11.3 and earlier, all variants	Unaffected	Unaffected	Unaffected	Unaffected
releases 12.0-based releases				
12.0	12.0 mainline	12.0(3b)	12.0(4), April 19, 1999*	12.0(4), April 19, 1999*
12.0S	ISP support: 7200, RSP, GSR12000. In field test.	–	12.0(4)S (treated as interim** and released to field testers on request only)	12.0(5)S June 21, 1999*
12.0T	12.0 new	12.0(3)T2,	12.0(4)T,	12.0(4)T,

	technology early deployment	April 14, 1999*	April 26, 1999*	April 26, 1999*
12.0DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)	–	–	Unaffected; not supported on affected platforms.
12.0(1)W5(x)	12.0 for Catalyst 8500 and LS1010	–	–	Unaffected; not supported on affected platforms.
12.0(0.6)W5	One-time early deployment for CH-OC12 module in Catalyst 8500 series switches	–	–	Unaffected; not supported on affected platforms.
12.0(1)XA3	Short-life release; merged to 12.0T at 12.0(2)T.	–	Merged	Upgrade to 12.0(3)T2 or 12.0(4)T
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0T at 12.0(3)T.	Unaffected	Merged	Unaffected; not supported on affected platforms. Regular upgrade path is via 12.0(4)T
12.0(2)XC	Short-life release for new features in Cisco 2600, Cisco 3600, ubr7200, ubr900 series; merged to	–	Merged	Upgrade to 12.0(3)T2 or 12.0(4)T

	12.0T at 12.0(3)T.			
12.0(2)XD	Short-life release for ISDN voice features; merged to 12.0T at 12.0(3)T.	–	Merged	Upgrade to 12.0(3)T2 or 12.0(4)T.
12.0(x)XE	Short-life release for selected enterprise features; merged to 12.0T at 12.0(3)T.	12.0(2)XE3, April 13, 1999*	Merged	Upgrade to 12.0(3)T2 or 12.0(4)T.
12.0(2)XF	Short-life spot release of 12.0 for the Catalyst 2900XL LAN switch; merged to 12.0T at 12.0(4)T.	Unaffected	Merged	Unaffected; not supported on affected platforms. Regular
12.0(2)XG	Short-life release for voice modules and features; merged to 12.0T at 12.0(4)T.	–	Merged	upgrade path is via 12.0(4)T. Upgrade to 12.0(4)T

* All dates are tentative and subject to change

** Interim releases are subjected to less internal testing and verification than are regular releases, may have serious bugs, and should be installed with great care.

Workarounds

This vulnerability may be worked around by changing the configuration to avoid using input access lists, by removing NAT from the configuration, or by separating NAT and filtering functions into different network devices or onto different interfaces. Each of these changes has significant installation-dependent complexity, and must be planned and executed with a full understanding of the implications of the change.

If the configuration of a router is changed to eliminate NAT, or to change the interfaces on which NAT is applied, as a means of avoiding this vulnerability, the router must be reloaded before the change will have the

desired effect.

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

Cisco knows of no public announcements or discussion of this vulnerability before the date of this notice. Cisco has had no reports of malicious exploitation of this vulnerability. However, the nature of this vulnerability is such that it may create security exposures without knowingly being "exploited" as the term is usually used with respect to security vulnerabilities.

This vulnerability was reported to Cisco by several customers who found it during in-service testing.

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-19990414-ios-nat-acl.shtml>. In addition to Worldwide Web posting, the initial version of this notice is being sent to the following e-mail and Usenet news recipients:

- cust-security-announce@cisco.com
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- firewalls@greatcircle.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	1999 April 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. This includes instructions for press inquiries regarding Cisco security notices.

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

Updated: Apr 14, 1999

Document ID: 13659
