

Cisco Security Advisory: Cisco IOS DFS Access List Leakage

Document ID: 13655

Advisory ID: cisco-sa-19981105-ios-dfs-acl

<http://www.cisco.com/warp/public/707/cisco-sa-19981105-ios-dfs-acl.shtml>

Revision 1.3

For Public Release 1998 November 05 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

Errors in certain Cisco IOS software versions for certain routers can cause IP datagrams to be output to network interfaces even though access lists have been applied to filter those datagrams. This applies to routers from the Cisco 7xxx family only, and only when those routers have been configured for distributed fast switching (DFS).

There are two independent vulnerabilities, which have been given Cisco bug IDs CSCdk35564 and CSCdk43862. Each vulnerability affects only a specialized subset of DFS configurations. Affected configurations are not believed to be extremely common, but neither are they extremely rare. More details of affected configurations are in the "Who is Affected" section of this document.

These vulnerabilities may permit users to send packets to parts of the customer's network for which they are not authorized. This may permit unauthorized access or other attacks on customer computer systems or data. Cisco does not know of any incidents in which these vulnerabilities have actually been exploited by attackers.

Neither vulnerability affects any Cisco product other than routers in the 70xx or 75xx series. Of 70xx routers, only routers with the optional route-switch processor (RSP) card are affected. Additional configuration conditions apply.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19981105-ios-dfs-acl.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

These vulnerabilities apply only to the Cisco 7xxx router family. The Cisco 7xxx family are large, rack-mounted backbone routers used primarily by Internet service providers and in large enterprise networks.

Cisco 75xx routers are affected by both vulnerabilities. Cisco 70xx routers are affected only if they have RSP cards installed. Cisco 72xx routers are not affected by either vulnerability; an earlier version of this notice erroneously mentioned 72xx routers, but affected hardware configurations are not possible on the 72xx platform, and DFS cannot be configured on 72xx routers.

CSCdk35564 affected configurations

CSCdk35564 is a defect in the 11.1CC and 11.1CT releases. Routers running Cisco IOS software versions other than 11.1CC and 11.1CT are not affected by CSCdk35564. Cisco 75xx routers are affected; Cisco 70xx routers are not supported with the affected hardware/software combinations.

Note: If you are a [registered CCO user](#) and you have logged in, you can view bug information.

- View [CSCdk35564](#)

To be affected by CSCdk35564, your router must be configured to switch traffic from an interface *with* DFS enabled to an interface *without* DFS enabled. This most commonly happens when routers contain both versatile interface processor (VIP) interface cards and non-VIP interface cards. Since DFS is supported only on VIP interfaces, traffic from a VIP to a non-VIP interface may be going from DFS to non-DFS.

CSCdk43862 affected configurations

CSCdk43862 affects 11.1, 11.2, and 11.3 versions of Cisco IOS software on the Cisco 70xx and 75xx series; see the table later in this document for details.

Note: If you are a [registered CCO user](#) and you have logged in, you can view bug information.

- View [CSCdk43862](#)

To be vulnerable, your router must be configured to switch traffic from an input interface with DFS enabled to a logical subinterface of a physical output interface. The output interface may or may not have DFS enabled; the important question for the output interface is whether or not subinterfaces are in use, and whether or not output traffic to subinterfaces is being filtered.

Products Confirmed Not Vulnerable

Although each of the vulnerabilities is different and manifests itself under different conditions, both involve DFS. DFS is not enabled by default in any Cisco product, and must be manually configured. If the command **ip route-cache distributed** does not appear in your router configuration file, then you are *not* affected by either vulnerability.

Specifically, process switching (**no ip route-cache**), ordinary fast switching (**ip route-cache**), optimum switching (**ip route-cache optimum**), and CEF or dCEF switching (**ip route-cache cef**, **ip cef distributed switch**) are *not* affected. Flow switching is considered a form of fast switching, and is affected only in

distributed mode. Interactions between flow switching and access lists reduce, but do not eliminate, the impact of both vulnerabilities when flow switching is enabled along with DFS.

If DFS is enabled on *all* of the interfaces in your router, then you are *not* affected by CSCdk35564. If DFS is not enabled on *any* interface in your router, then you are *not* affected. If you do not use the **ip access-group** command to filter outgoing traffic on any non-DFS interfaces, then you are *not* affected.

Subinterfaces are pseudo-interfaces associated with subsets of the traffic on physical interfaces. For instance, a physical Frame Relay interface might have a subinterface associated with each Frame Relay PVC. Subinterfaces do not exist by default; they are created as part of user configuration. Subinterface numbers always contain periods, as in "Serial 0/1.1". If your configuration file does not contain any such "dotted" interface numbers, then you are *not* vulnerable.

If you do not use the **ip access-group** command to apply output access-list filtering to *subinterfaces*, then you are *not* vulnerable.

CSCdk43862 causes the access list applied to one subinterface on a physical interface to be incorrectly used for traffic destined for a different subinterface. If you use the *same* access list to filter outbound traffic on *all* subinterfaces of any given physical interface, then you are *not* vulnerable.

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

Details

CSCdk43862 has a duplicate report, CSCdk43696. The bug ID CSCdk43862 should be used to refer to this defect.

Impact

Incorrect access-list filtering may be applied to output packets. Output access lists are frequently used to implement security filtering, and the failure of such access lists may permit users to send packets to parts of the network for which they are not authorized. This, in turn, may permit them to bypass security restrictions, and to gain access to data or resources from which they should be excluded.

Neither of the defects described in this notice "fails reliably". The same access lists, on the same interfaces, may work correctly at some times, and fail at other times. Because of this, administrators who test their access lists may be misled into believing that the access lists are providing effective protection, when in fact they are not.

CSCdk43862 may result in legitimate traffic being filtered out, as well as in undesired traffic being permitted to pass through the router. CSCdk35564 never filters legitimate traffic; it only permits undesired traffic.

An attacker who had detailed knowledge of these vulnerabilities might be able to create conditions favorable to unauthorized access being permitted. However, such activity would probably be unnecessary; even without deliberate intervention by an attacker, such conditions would be expected to occur frequently during the operation of most affected networks.

Software Versions and Fixes

The following table summarizes the affected Cisco IOS software versions for both CSCdk35564 and CSCdk43862, and indicates which versions have been fixed. To use the table, look up the software release you're currently running (available from the **show version** command on your router) in the first column of the

table. The other columns of the table tell you which Cisco IOS software versions from your major release have been fixed, and which versions Cisco recommends you install.

The table lists both interim versions and regular released versions. Interim versions receive far less testing, and are generally of less certain quality, than regular released versions. Cisco recommends installing regular released software whenever possible. Interim versions are listed for reference, and for the convenience of customers who must upgrade before appropriate regular released versions are available.

As always, a fix applied to one regular released version in a major release means that all later versions of that major release are also fixed. For instance, 11.2(17) is fixed, so 11.2(18) and later are also fixed.

The table is designed to cover all supported software on all affected Cisco routers. If you are running distributed fast switching on a 75xx router, or a 70xx router with an RSP processor, and you are using an 11.1, 11.2, or 11.3 release not listed in the table, please contact the Cisco TAC for assistance.

Cisco IOS Major Release (only 7xxx releases are listed)	Initial CSCdk35564 Fixes		Initial CSCdk43862 Fixes		Upgrade Path for 7xxx DFS
	Interim (minimal testing;	Regular (dates are	Interim (minimal testing;	Regular (dates are	
11.0 and earlier, all variants	urgent upgrades only)	subject to change)	urgent updates only)	subject to change)	Users
	Unaffected	Unaffected	Unaffected	Unaffected	Unaffected
11.1	Unaffected	Unaffected			Go to 11.1CA
11.1CA (core ED)	Unaffected	Unaffected	11.1(22)CA	11.1(22)CA	11.1(22)CA
11.1CC (CEF ED)	11.1(21.2)CC	11.1(21)CC1 11.1(22)CC	11.1(21.2)CC	11.1(21)CC1 11.1(22)CC	or later 11.1(21)CC1, 11.1(22)CC or later
11.1CT (tag switch ED)	11.1(21.2)CT	11.1(22)CT	11.1(21.2)CT	11.1(22)CT	11.1(22)CT or later
11.2	Unaffected	Unaffected	11.2(16.1)	11.2(17), planned Jan-1999	11.2(17) or later; 11.2(16.1) or 11.3 if 11.2(17) schedule unacceptable
11.2F	Unaffected	Unaffected			Go to 11.3
11.2P (platform ED)	Unaffected	Unaffected	11.2(16.1)P	11.2(17)P, planned Jan-1999	11.2(17)P or later; 11.2(16.1)P or 11.3 if 11.2(17)P schedule

					unacceptable.
11.2BC (CIP ED)	Unaffected	Unaffected	11.2(16.1)BC	11.2(17)BC, planned Jan–1999	11.2(17)BC or later; 11.2(16.1)BC if 11.2(17)BC schedule unacceptable.
11.3	Unaffected	Unaffected	11.3(6.2)	11.3(7), planned Nov–1998	11.3(7) or later
11.3T	Unaffected	Unaffected	11.3(6.2)T	11.3(7)T, planned Nov–1998	11.3(7)T or later
11.3NA (voice ED)	Unaffected	Unaffected	11.3(6.2)NA	11.3(7)NA, Planned Dec–1998	11.3(7)NA or later; 11.3(6.2)NA if 11.3(7)NA schedule unacceptable.
11.3(2)XA	Unaffected	Unaffected	–	–	11.3(7) or later
12.0(1) and later, all variants	Unaffected	Unaffected	Unaffected	Unaffected	Unaffected

Because of restricted port adapter support, Cisco does not believe that many, if any, customers are using DFS with 11.1 mainline software. 11.1CA is recommended for both functionality and stability reasons.

The 11.1(21)CC1 release is a special release of 11.1CC; the 11.1CC release sequence runs from 11.1(21)CC through 11.1(21)CC1, then to 11.1(22)CC.

11.3(2)XA was a special one–time release based on 11.3(2). The functionality of 11.3(2)XA was carried into the 11.3(3) release.

Workarounds

These vulnerabilities can be worked around by disabling DFS on network interfaces (with **no ip route–cache distributed**). Be aware that the purpose of DFS is to transfer computational load from the router's primary CPU to the CPUs on the VIP cards, and that disabling DFS may therefore cause overload of the primary CPU. Evaluate your traffic load and CPU usage before using this workaround.

If all interfaces in the router are DFS–capable, but DFS has for some reason been enabled only on some of the interfaces, it may be possible to work around CSCdk35564 by enabling DFS on all interfaces. This will not affect CSCdk43862.

CSCdk43862 can sometimes be worked around by reconfiguring to use the same output access list on all the subinterfaces of a physical interface.

Another possible workaround is to redesign the access lists structure on the router to avoid the need for output access lists on affected interfaces.

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 these vulnerabilities prior to the date of this notice.

CSCdk35564 was found by a Cisco customer during installed-system testing. CSCdk43862 was found by Cisco during internal testing.

Because of the nature of these vulnerabilities, attackers would rarely be expected to exploit them directly. In most cases, attackers would simply find themselves with access to network resources to which administrators thought they had denied access. Cisco has had no actual reports of malicious attacks succeeding because of this vulnerability, nor of anyone deliberately trying to create "vulnerable" conditions.

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-19981105-ios-dfs-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)
- first-info@first.org
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- nanog@merit.edu
- Various internal Cisco mailing lists

Future updates of this advisory, 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 above URL for any updates.

Revision History

Revision 1.3	1998-November-05	Initial public release.
--------------	------------------	-------------------------

Cisco Security Procedures

Please report security issues with Cisco products, and/or sensitive security intrusion emergencies involving Cisco products, to security-alert@cisco.com. Reports may be encrypted using PGP; public RSA and DSS

keys for "security-alert@cisco.com" are on the public PGP key servers.

The alias "security-alert@cisco.com" is used only for reports incoming to Cisco. Mail sent to the list goes only to a very small group of users within Cisco. Neither outside users nor unauthorized Cisco employees may subscribe to "security-alert@cisco.com".

Please do not use "security-alert@cisco.com" for configuration questions, for security intrusions that you do not consider to be sensitive emergencies, or for general, non-security-related support requests. We do not have the capacity to handle such requests through this channel, and will refer them to the TAC, delaying response to your questions. We advise contacting the TAC directly with these requests. TAC contact numbers 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

All formal public security notices generated by Cisco are sent to the public mailing list "cust-security-announce@cisco.com". For information on subscribing to this mailing list, send a message containing the single line "info cust-security-announce" to "majordomo@cisco.com". An analogous list, "cust-security-discuss@cisco.com" is available for public discussion of the notices and of other Cisco security issues.

Press Contacts

Press inquiries regarding Cisco security notices should be directed to Doug Wills, dwills@cisco.com, +1 408 527 9475.

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

Updated: Nov 23, 1998

Document ID: 13655
