

# Cisco Security Advisory: Cisco PIX and CBAC Fragmentation Attack

Document ID: 23885

Advisory ID: cisco-sa-19980910-pix-cbac-nifrag

<http://www.cisco.com/warp/public/707/cisco-sa-19980910-pix-cbac-nifrag.shtml>

## Revision 1.2

Last Updated 1998 September 11 1500 UTC (GMT)

For Public Release 1998 September 10 1500 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

Neither Cisco's PIX Firewall, nor the Context-Based Access Control (CBAC) feature of Cisco's IOS Firewall Feature Set, protects hosts against certain denial of service attacks involving fragmented IP packets. This vulnerability does not permit network "breakins". The vulnerability is most severe in configurations involving static Network Address Translation (NAT) entries, or in configurations not involving any use of NAT.

The vulnerability is present in Cisco PIX Firewall software up to and including version 4.2(1), and in CBAC versions of Cisco IOS software through 11.2P and 11.3T, and will be present in initial 12.0 revisions of CBAC software.

The Cisco Centri Firewall does not share this vulnerability.

Stateless packet filtering products, such as the extended access lists available in non-CBAC versions of Cisco IOS software, share the vulnerability because of the inherent limitations of stateless operation. This it is not considered a defect in stateless filtering. More information is in the section on "Stateless Packet Filters" in this document.

This vulnerability will be fixed in Cisco PIX Firewall software version 4.2(2), which is tentatively scheduled

for release on or after September 16, 1998. The vulnerability is scheduled to be fixed for CBAC in Cisco IOS software release 12.0(2) and 12.0(3)T, which are tentatively scheduled for release in late November 1998, and in late January 1999, respectively. All schedules are subject to change.

The possibility of IP fragmentation attacks against packet filters, from Cisco and other vendors, has been widely known for a very long time. However, exploitation does not seem to be increasing. Therefore, Cisco does not believe that the majority of its customers are critically exposed by this vulnerability. Cisco is, however, prepared to support any customers who suffer actual attacks, or who have specific reason to think that they are likely to be attacked in this way.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-19980910-pix-cbac-nifrag.shtml>.

## Affected Products

This section provides details on affected products.

### Vulnerable Products

Cisco PIX Firewalls with software versions up to and including 4.2(1) are affected. CBAC feature on Cisco IOS software versions up to and including 11.2P and 11.3T (all edit levels), as well as 12.0 versions and 12.0T versions up to and including 12.0(1) and 12.0(2)T, are also affected.

A similar vulnerability affects all users who rely on stateless packet filtering products, from Cisco or any other vendor. The packet filters affected are those which are capable of filtering based on information, such as TCP or UDP port numbers, that may not be present in every fragment of a datagram. This vulnerability is not considered a defect for a stateless packet filtering product.

Packet filtering using non-CBAC Cisco IOS software extended access lists falls into this category of stateless filtering, and such access lists are vulnerable in all versions of Cisco IOS software. The affected extended access lists are numbered lists from 100–199, or named access lists created with the **extended** keyword. Non-extended Cisco IOS access lists, numbered from 1–99, are not capable of filtering on port numbers, and are not affected.

### Products Confirmed Not Vulnerable

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

## Details

This section provides detailed information about these vulnerabilities.

### PIX Firewall

This vulnerability on the PIX Firewall has been assigned Cisco bug ID CSCdk36273.

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

[View CSCdk36273](#) ([registered](#) customers only)

### Problem Description for the PIX Firewall

PIX Firewall software up through version 4.2(1) will pass any non-initial fragment destined for any host for which either a static or a dynamic NAT table entry exists. Static NAT table entries are created with the PIX Firewall **static** command, and dynamic entries are created by inside hosts initiating IP traffic exchanges with outside hosts. No checks are made as to whether or not non-initial fragments belong to actual existing connections, so it is possible for any outside host to send fragments to any inside host that has a NAT entry, regardless of whether or not there is a connection between the two hosts, and regardless of whether a conduit is configured.

### **Immediate Response for the PIX Firewall**

The following changes have been made to the behavior of the PIX Firewall for version 4.2(2):

- Interfragment state is now being kept. Any non-initial fragment will be discarded unless the corresponding initial fragment was permitted to pass through the firewall. Non-initial fragments received before the corresponding initial fragments will be discarded.  
This eliminates the possibility of overloading host resources with unmatched non-initial fragments, and requires attackers to use relatively elaborate address spoofing for attacks using unmatched initial fragments.  
This change may have undesirable effects in certain cases, since it will result in the firewall's discarding any datagram whose fragments arrive out of order. There are a number of circumstances that may cause out-of-order delivery of legitimate fragments. Cisco therefore advises caution in installing the new software, although Cisco does not believe that legitimate out-of-order fragmented traffic (or indeed fragmented traffic of any kind) is common at Internet firewalls.
- Fragments received for hosts without conduits are discarded unless those fragments can be matched with active connections. Matching is performed using IP source and destination address and protocol type.
- The amount of memory dedicated to fragmentation state is limited in order to reduce the chance of denial of service attacks against the PIX Firewall itself. Fragmentation state is created only in response to initial fragments, and is kept until either all fragments of the datagram in question have been processed, or a timeout expires. Initial fragments received when fragmentation state resources are exhausted are discarded.  
Unfragmented traffic will never be discarded because of lack of fragment state memory. Even when the system is under heavy attack with fragmented packets, legitimate fragmented traffic, if any, will still get some fraction of the firewall's fragment state resources, and legitimate unfragmented traffic will flow unimpeded.

These or equivalent changes will be carried forward into all PIX Firewall software versions after version 4.2(2).

### **Getting Fixed Software for the PIX Firewall**

Cisco is offering free upgrades to 4.2(2) software for all PIX Firewall customers, regardless of service contract status. The upgrades will be available as soon as the 4.2(2) software has been released.

Once the software has been released, customers with service contracts may download it from Cisco's Worldwide Web site.

Customers without service contracts should get their upgrades by contacting the Cisco 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](mailto:tac@cisco.com)

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. Please do *not* contact either "psirt@cisco.com" or "security–alert@cisco.com" for software upgrades.

As with any new software installation, PIX Firewall customers planning to upgrade to version 4.2(2) should carefully read the release notes and other relevant documentation before beginning any upgrade.

### **Long–term Plans for the PIX Firewall**

Cisco is evaluating the possibility of making additional changes in PIX Firewall fragment handling, with the intention of closing additional fragmentation–related vulnerabilities. If further changes are made, they are likely to be of a relatively major nature, and therefore will probably appear in a PIX Firewall release after release 4.2.

### **Workarounds for the PIX Firewall**

Although there are no direct workarounds for this vulnerability, customers can reduce their exposure by avoiding reliance on static NAT entries. Hosts actively using dynamic NAT will remain vulnerable to some degree until fixed software is installed. However, exploiting the vulnerability against dynamically allocated addresses is more difficult than exploiting it against statically allocated addresses. To exploit the vulnerability via dynamic NAT, an attacker must do extra work to determine which dynamic addresses are active at any given time, and to which hosts those active addresses correspond.

## **CBAC (Cisco IOS Firewall Feature Set) Details**

This vulnerability in the CBAC feature has been assigned Cisco bug ID CSCdk41516.

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

[View CSCdk41516](#) ([registered](#) customers only)

### **Problem Description for CBAC**

The Cisco IOS CBAC feature, up through all 11.2– and 11.3–based versions including 11.2P and 11.3T, and up through 12.0–based versions through 12.0(1) and 12.0(2)T, does no filtering of non–initial IP fragments. The CBAC feature performs much of its filtering by dynamically modifying extended IP access lists, and, as with all Cisco IOS extended access lists, the access lists modified by CBAC always pass non–initial fragments.

### **Immediate Response for CBAC**

The following changes will be made to the behavior of the CBAC feature, and are presently targeted for versions 12.0(2) and 12.0(3)T:

- Interfragment state will be kept. Any non–initial fragment will be discarded unless the corresponding initial fragment was permitted to pass through the firewall. Non–initial fragments received before the corresponding initial fragments will be discarded.

This applies only to packets being processed by CBAC as configured with the **ip inspect** configuration commands; fragmentation state checks will not be applied to router traffic not being inspected by CBAC, even if that traffic is filtered with access lists.

This change eliminates the possibility of overloading host resources with unmatched non–initial fragments, and requires attackers to use relatively elaborate address spoofing for attacks using unmatched initial fragments.

This change may have undesirable effects in certain cases, since it will result in the firewall's

discarding any packet whose fragments arrive out of order. There are a number of circumstances that may cause out-of-order delivery of legitimate fragments. Because routers running Cisco IOS software are used in a very large variety of networks, and because the CBAC feature is often used to isolate parts of internal networks from one another, the new behavior will not be enabled by default. Fragment checking must be explicitly enabled using the **ip inspect name inspect-name fragment** configuration command. Cisco recommends that this command be used whenever CBAC is being used as an Internet firewall, unless there are special circumstances that dictate otherwise. Cisco believes that legitimate out-of-order fragments are rare at Internet firewalls.

- The amount of memory dedicated to fragmentation state is limited in order to reduce the chance of denial of service attacks against the firewall router itself. Fragmentation state is created only in response to initial fragments, and is kept until either all fragments of the datagram in question have been processed, or a timeout expires. Initial fragments received when fragmentation state resources are exhausted are discarded.

Unfragmented traffic will never be discarded because of lack of fragment state memory. Even when the system is under heavy attack with fragmented packets, legitimate fragmented traffic, if any, will still get some fraction of the firewall's fragment state resources, and legitimate unfragmented traffic will flow unimpeded.

- Fragment lengths will be checked for legality, and fragment offsets will be checked to avoid port-number overwrite attacks. This offset check duplicates the check already applied by extended access lists, for those unusual configurations where CBAC is being used without access lists.

These or equivalent changes will be carried forward into all future versions of the Cisco IOS Firewall Feature Set.

### Getting Fixed Software for CBAC

Cisco is offering free upgrades to all customers who have purchased the Cisco IOS Firewall Feature set, regardless of service contract status. Since there is no defect in stateless packet filtering, this free upgrade program does not apply to customers who have purchased only non-firewall Cisco IOS.

When the updated software has been released, customers with service contracts should obtain Cisco IOS software updates through their usual channels. Customers with service contracts purchased from Cisco or from most resellers may download updates from Cisco's Worldwide Web site.

Customers without service contracts should get their upgrades by contacting the Cisco 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](mailto:tac@cisco.com)

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. Please do *not* contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

As with any new software installation, customers planning to upgrade should carefully read the release notes and other relevant documentation before beginning any upgrade. Also, it is important to be certain that the new version of Cisco IOS software is supported by your hardware, and especially that enough DRAM is available.

### Long-term Plans for CBAC

Cisco is evaluating the possibility of making additional changes in Cisco IOS Firewall Feature Set fragment handling, with the intention of closing additional fragmentation-related vulnerabilities. If further changes are

made, they are likely to be of a relatively major nature, and therefore will probably appear in a Cisco IOS software release after release 12.0.

## Workarounds for CBAC

There are no CBAC workarounds specific to this vulnerability. However, customers may be able to reduce their exposure by using dynamic NAT. Also, non-extended IP access lists can filter IP fragments, and may be useful in controlling potential attacks in some configurations.

## Stateless Packet Filters

A stateless IP packet filter, such as a traditional access list in Cisco IOS software, must make all of its forwarding decisions for any specific packet based only on information in that packet. If the filtering is based on criteria such as TCP or UDP port numbers, the necessary information is typically present only in the initial fragment of a fragmented datagram. It is therefore impossible to tell if a non-initial fragment is part of a forbidden datagram or of a permitted one. Therefore, stateless packet filters that use such criteria must pass all, or substantially all, non-initial fragments. Such filters rely on blocking of initial fragments to prevent completed delivery of any forbidden datagrams. This makes them vulnerable to the fragmentation denial of service attacks discussed in this notice.

Extended access lists in Cisco IOS software can filter based on TCP and UDP port numbers, as well as based on ICMP packet types, and therefore fall into the vulnerable category. A Cisco IOS software extended access list will pass any non-initial fragment of a fragmented IP datagram.

Stateless packet filters that do not use information such as port numbers do not suffer from this vulnerability, since all the information used by such filters is present in every fragment of a datagram. Cisco IOS software's *non-extended* access lists do not match on port numbers. They therefore can (and do) filter non-initial fragments as well as initial fragments.

Vulnerability to fragmentation attacks is a well-known and largely inherent limitation of stateless IP packet filtering. Cisco does not consider this a defect in its stateless packet filtering products, and plans no immediate response for those products. Although Cisco may in the future choose to improve the fragment handling in its stateless filtering products, there is no way to completely prevent an attacker from constructing fragments that will pass any given stateless packet filter if the filtering criteria include port numbers. There is therefore no way to entirely avoid fragmentation-based denial of service attacks using such a filter.

## Impact

Even though the firewall keeps an attacker from making actual connections to a given host, he or she may still be able to disrupt services provided by that host. This is done by sending many unmatched non-initial IP fragments, which use reassembly resources on the target host. Hosts vary widely in the quality of their resource management and in their response to this attack. Some hosts can be made nearly useless by traffic levels that might realistically be available to attackers.

The attack can be launched only against hosts to which the attackers can address packets. If dynamic NAT is being used, attack packets can be sent only to hosts which are actively communicating with the Internet, since NAT translation table entries will not exist for other hosts.

Because the firewall drops only the initial fragments of blocked datagrams, attackers can exploit this vulnerability by sending streams of complete fragmented packets. The attacker in this case deliberately intends the initial fragments to be blocked by the firewall. Since only the non-initial fragments will be forwarded, the effect on the target host will be similar to the effect of sending only the non-initial fragments to begin with. This method involves some waste of the attacker's resources, and is therefore slightly less

effective than simply sending the non-initial fragments alone. This method is of interest because it allows attacks to be launched using relatively standard networking tools, without any special exploit program.

## 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.

For more information about software versions and fixes, see [Details](#).

## Workarounds

For information about workarounds, see [Details](#).

## 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](mailto: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 is common to numerous packet filtering devices, both stateful and stateless, from Cisco and other vendors. This vulnerability is a well-known one in the area of router-based stateless packet filtering, and is occasionally exploited by attackers when stateless filters are in use. Exploitation against stateful filters such as the PIX Firewall and CBAC may reasonably be expected to occur from time to time.

Because it is possible to exploit this vulnerability "by accident" with packet floods of various sorts, this vulnerability probably causes some number of problems in cases where even the attackers themselves do not fully understand the mechanism by which they are damaging their targets, as well as in cases where the attackers have deliberately decided to target this specific problem.

Cisco knows of no organized, systematic exploitation specific to this vulnerability, but flooding attacks that could exercise it are reasonably common events on the Internet. Such flooding attacks cause a wide range of negative responses in targeted networks, and this vulnerability represents one of those negative responses.

Flooding tools capable of exploiting this vulnerability are widely available. Special-purpose tools designed to selectively exploit this vulnerability seem relatively uncommon, but Cisco has not conducted a thorough search for such tools. Such a tool would be easy for a moderately sophisticated network programmer to produce.

This vulnerability has been publicly discussed with specific reference to the Cisco PIX Firewall on the BUGTRAQ mailing list, beginning in late August of 1998. There have been many other discussions in other public forums regarding this vulnerability as it applies to packet filters in general, and it is reasonable to suppose that there may have been public discussions of this vulnerability as applied specifically to Cisco products. This vulnerability should be considered to be widely known in both the computer security community and the "cracker" community.

## 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-19980910-pix-cbac-nifrag.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](mailto:cust-security-announce@cisco.com)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [first-info@first.org](mailto:first-info@first.org)
- 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 1.2	<del>1998-September-11</del>	Corrected PIX release date
Revision 1.1	<del>1998-September-11</del>	yet again REAL initial released version; corrected PIX release date
Revision 1.0	<del>1998-September-10</del>	Initial released version

## Cisco Security Procedures

Please report security issues with Cisco products, and/or sensitive security intrusion emergencies involving Cisco products, to [security-alert@cisco.com](mailto: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](mailto: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.

---

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

---

Updated: Sep 11, 1998

Document ID: 23885

---