

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of Multiple IOS IPS Vulnerabilities

Document ID: 81817

<http://www.cisco.com/warp/public/707/cisco-amb-20070213-iosips.shtml>

Revision 1.0

For Public Release 2007 February 13 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

[Cisco Response](#)
[Device-Specific Mitigation and Identification](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)
[Related Information](#)

Cisco Response

Vulnerability Characteristics

The Cisco Intrusion Prevention System (IPS) feature set of Cisco IOS contains the following vulnerabilities:

1. Fragmented Packet Evasion Vulnerability – This vulnerability can be exploited remotely without authentication and no user interaction is necessary. The attack vector is through the use of fragmented IP packets. This vulnerability is not designated by a CVE ID. By fragmenting malicious network traffic, it may be possible to evade detection by IPS signatures which utilize regular expressions to identify attacks.
2. ATOMIC.TCP Regular Expression Denial of Service Vulnerability – This vulnerability can be exploited remotely without authentication and no user interaction is necessary. The attack vector is through the use of IP traffic that triggers signature 3123.0 (NetBus Pro Traffic). This vulnerability is not designated by a CVE ID. Certain network traffic can trigger IPS signatures which use the regular expression feature of the ATOMIC.TCP signature engine possibly resulting in the failure of the IOS IPS device. Signature 3123.0 (NetBus Pro Traffic) has been demonstrated to trigger this vulnerability. The most effective workaround (as described in the PSIRT Security Advisory) is to disable signature 3123.0 within the IOS IPS configuration. In addition, there is network mitigation/identification information included in this Applied Mitigation Bulletin for this vulnerability.

Note: This vulnerability may affect any IPS signature using the regular expression functionality of the ATOMIC.TCP engine. Currently, Cisco only ships one signature configured this way (3123.0). If custom signatures have been added to an IOS IPS device configured use the ATOMIC.TCP engine with a regular expression, the only workaround is to delete these signatures from the IPS configuration. The network mitigation/identification information contained in this document only applies to the use of Signature 3123.0.

This document contains information to assist Cisco customers in identifying and mitigating attempts to exploit the Multiple IOS IPS Vulnerabilities.

Information about vulnerable, unaffected and fixed software is available in the PSIRT Security Advisory: <http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.shtml>.

Mitigation Technique Overview

Cisco devices provide several countermeasures for the Multiple IOS IPS Vulnerabilities. The most preventive control is provided by IOS Access Control Lists (ACLs) and Fragment Reassembly by PIX, ASA and FWSM firewalls at the network level. Detective controls can be performed through syslog messages and access control list **show** commands.

The effectiveness of any mitigation technique 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 is the most appropriate for use in the intended network before it is deployed.

Device-Specific Mitigation and Identification

Specific information on mitigation and identification is available for these devices:

- [Cisco IOS Routers](#)
- [Cisco ASA, PIX and FWSM Firewalls](#)
- [Cisco IOS Switches](#)



Caution: The effectiveness of any mitigation technique is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. As with any configuration change, evaluate the impact of this configuration prior to applying the change.

Cisco IOS Routers

Mitigation: Fragmented Packet Evasion Vulnerability

Transit Access Control Lists (tACLs)

To mitigate the effects of the fragmented packet evasion vulnerability on the IOS IPS device, Transit Access Control Lists (tACLs) can be used on devices that filter traffic destined for IOS IPS inspection by the vulnerable IOS IPS device. The **fragments** keyword of IOS Transit Access Control Lists (ACL) can be used to prohibit fragmented IP packets from entering the vulnerable IOS IPS device.

ACLs have a fragments keyword that enables specialized fragmented packet-handling behavior. In general, noninitial fragments that match the Layer 3 statements (protocol, source address, and destination address) are affected by the permit or deny statement of the matched entry. This Layer 3 matching is independent of the Layer 4 information in an ACL. Note that the use of the fragments keyword can force ACLs to either deny or permit noninitial fragments with more granularity.

Because many attacks rely on flooding with fragmented packets, filtering fragments coming into the internal network provides an added measure of protection and helps ensure that an attack cannot inject fragments by

simply matching Layer 3 rules in the transit ACL.

Refer to [Access Control Lists and IP Fragments](#) for a detailed discussion of the options.

For more information on Transit ACLs, refer to [Transit Access Control Lists: Filtering at Your Edge](#).

The following Transit ACL denies all IP packets containing non-initial fragments sent to the internal network 192.168.1.0/24.

Note: It is recommended that the **deny fragments** entries be included at the beginning of the ACL. If they are not, due to the lack of Layer 4 checks with packets containing fragments, these fragmented packets could bypass the **deny** entries if these packets are permitted earlier in the ACL based on just Layer 3 information.

```
!  
  
!-- Deny all TCP/UDP/ICMP traffic sent to internal address  
!-- space (192.168.1.0/24) that consists  
!-- of non-initial fragments.  
  
!  
ip access-list extended fragments  
deny tcp any 192.168.1.0 0.0.0.255 fragments  
deny udp any 192.168.1.0 0.0.0.255 fragments  
deny icmp any 192.168.1.0 0.0.0.255 fragments  
deny ip any 192.168.1.0 0.0.0.255 fragments  
!  
  
!-- Permit/Deny all other Layer 3 and Layer 4 traffic in accordance  
!-- with existing security policies and configurations.  
  
!  
  
!-- Apply tACL to FastEthernet0 interface in the inbound direction.  
  
!  
interface FastEthernet0  
ip address 192.168.131.100 255.255.255.0  
ip access-group fragments in
```

Identification: Fragmented Packet Evasion Vulnerability

Transit Access Control Lists (tACLs)

The **show access-list [ACL name]** command can be used to display output indicating which entries in the ACL have denied packets. The following example indicates that the ACL dropped **103 TCP packets** that contained noninitial fragments and that were destined for the 192.168.1.0/24 network.

```
router-01#show access-list fragments  
Extended IP access list fragments  
 10 deny tcp any 192.168.1.0 0.0.0.255 fragments (103 matches)  
 20 deny udp any 192.168.1.0 0.0.0.255 fragments  
 30 deny icmp any 192.168.1.0 0.0.0.255 fragments  
 40 deny ip any 192.168.1.0 0.0.0.255 fragments  
router-01#
```

Mitigation: ATOMIC.TCP Regular Expression Denial of Service Vulnerability

Transit Access Control Lists (tACLs)

In order to mitigate the effects of the ATOMIC.TCP Regular Expression DoS vulnerability on the IOS IPS device, Transit Access Control Lists (tACLs) can be used on devices that filter traffic destined for IOS IPS inspection by the vulnerable IOS IPS device. Since this vulnerability is exploited by triggering IOS IPS Signature 3123.0 (NetBus Pro Traffic) and this signature looks for traffic on TCP/20034 it is possible to use tACLs to filter on traffic destined for internal address space on TCP/20034.

Note: NetBus Pro runs by default on TCP port 20034, but can be configured to run on other ports. For more information on tACLs, refer to [Transit Access Control Lists: Filtering at Your Edge](#).

The following tACL denies all TCP packets using TCP destination port 20034 sent to the internal network 192.168.1.0/24.

```
!  
  
!-- Deny connections on TCP port 20034 sent to internal address space (192.168.1.0/24).  
  
!  
ip access-list extended atomic-tcp  
  deny tcp any 192.168.1.0 0.0.0.255 eq 20034  
  permit ip any 192.168.1.0 0.0.0.255  
!  
  
!-- Permit/Deny all other Layer 3 and Layer 4 traffic in accordance  
!-- with existing security policies and configurations.  
  
!  
  
!-- Apply tACL to FastEthernet0 interface in the inbound direction.  
  
!  
interface FastEthernet0  
ip address 192.168.131.100 255.255.255.0  
ip access-group atomic-tcp in  
!
```

Identification: ATOMIC.TCP Regular Expression Denial of Service Vulnerability

Transit Access Control Lists (tACLs)

The **show access-list [ACL name]** command can be used to display output indicating which entries in the ACL have denied packets. The following example indicates that the ACL dropped **6 TCP/20034** packets that were destined to the 192.168.1.0/24 network.

```
router-01#show access-list atomic-tcp  
  
Extended IP access list atomic-tcp  
  10 deny tcp any 192.168.1.0 0.0.0.255 eq 20034 (6 matches)  
  20 permit ip any 192.168.1.0 0.0.0.255  
router-01#
```

Cisco ASA, PIX and FWSM Firewalls

Mitigation: Fragmented Packet Evasion Vulnerability

Fragment Reassembly

By default, the ASA, PIX 7.x and FWSM firewalls allow up to 24 fragments per full IP packet and up to 200 fragments awaiting reassembly. The firewall will reassemble these fragments by default in order to perform additional operations on the full IP packet. Reassembly causes the packets to be forwarded unfragmented to their destination, mitigating the impact of the vulnerability.

To prevent the sending of any fragments through the firewall, enter the following command:

```
firewall(config)#fragment chain 1 [interface_name]
```

Enter an interface name to prevent fragmentation on a specific interface. By default, this command applies globally to all interfaces.

Note: Setting the limit to **1** means that all packets must be whole, that is unfragmented. If fragmented traffic must be allowed between clients and servers, perhaps due to NFS traffic or small MTU sizes (such as those used for WAN interfaces), the chain keyword might require additional tuning. Setting the size limit to a large value can make the firewall more vulnerable to a DoS attack that employs fragment flooding.

The default values for the **fragment** command are as follows:

- chain is 24 packets
- interface is all interfaces
- size is 200
- timeout is 5 seconds

For more information on the **fragment** command reference the following:

- [ASA Fragment Command](#)
- [Configuring the Fragment Size on the FWSM](#)

Identification: Fragmented Packet Evasion Vulnerability

Fragment Reassembly

Cisco ASA, PIX and FWSM firewalls will generate syslog messages if they receive more fragments than they are configured to reassemble (using the **fragment chain [Maximum number of elements in a fragment set]** command). The following is an example of this syslog message generated by an FWSM when the attacker (IP = 192.168.30.50) attempts to send too many fragments to the destination host (IP = 192.168.1.1):

```
Jan 29 2007 13:20:15: %FWSM-4-209005: Discard IP fragment set with  
more than 2 elements: src = 192.168.30.50, dest = 192.168.1.1, proto = icmp,  
id = 62715
```

Reference the following entries for more information:

- [FWSM Syslog Message 209005](#)
- [ASA/PIX Syslog Message 209005](#)

Cisco IOS Switches

Mitigation: Fragmented Packet Evasion Vulnerability

Transit Access Control Lists (tACLs)

To mitigate the effects of the fragmented packet evasion vulnerability on the IOS IPS device, Transit Access Control Lists (tACLs) can be used on devices that filter traffic destined for IOS IPS inspection by the vulnerable IOS IPS device. The **fragments** keyword of IOS tACLs can be used to prohibit fragmented IP packets from entering the vulnerable IOS IPS device.

ACLs have a fragments keyword that enables specialized fragmented packet-handling behavior. In general, noninitial fragments that match the Layer 3 statements (protocol, source address, and destination address) are affected by the permit or deny statement of the matched entry. This Layer 3 matching is independent of the Layer 4 information in an ACL. Note that the use of the fragments keyword can force ACLs to either deny or permit noninitial fragments with more granularity.

Because many attacks rely on flooding with fragmented packets, filtering fragments coming into the internal network provides an added measure of protection and helps ensure that an attack cannot inject fragments by simply matching Layer 3 rules in the tACL.

Note: It is recommended that the deny fragments entries be included at the beginning of the ACL. If they are not, due to the lack of Layer 4 checks with packets containing fragments, these fragmented packets could bypass the deny entries if these packets are permitted earlier in the ACL based on just Layer 3 information.

Refer to [Access Control Lists and IP Fragments](#) for a detailed discussion of the options.

For more information on tACLs, refer to [Transit Access Control Lists: Filtering at Your Edge](#).

The following example shows an IOS switch tACL with entries to prevent packets with non-initial fragments destined for the 192.168.1.0/24 network.

```
ip access-list extended deny-fragments
deny tcp any 192.168.1.0 0.0.0.255 fragments
deny udp any 192.168.1.0 0.0.0.255 fragments
deny icmp any 192.168.1.0 0.0.0.255 fragments
deny ip any 192.168.1.0 0.0.0.255 fragments
!

!-- Permit/Deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations.

!

!-- Apply tACL to VLAN interface in the outbound direction.

!
interface Vlan20
ip address 192.168.1.2 255.255.255.0
ip access-group deny-fragments out
!
```

Identification: Fragmented Packet Evasion Vulnerability

Transit Access Control Lists (tACLs)

The **show access-list [ACL name]** command can be used to display output indicating which entries in the ACL have denied packets. The following example indicates that a total of **10 ICMP packets** with noninitial fragments were prevented from reaching the 192.168.1.0/24 network. As indicated above, the access list has been applied in the outbound direction for packets destined to VLAN 20 (192.168.1.0/24).

```
cat6k-01#show access-lists deny-fragments
Extended IP access list deny-fragments
 10 deny tcp any 192.168.1.00 0.0.0.255 fragments
 20 deny udp any 192.168.1.00 0.0.0.255 fragments
 30 deny icmp any 192.168.1.00 0.0.0.255 fragments (10 matches)
 40 deny ip any 192.168.1.00 0.0.0.255 fragments
cat6k-01#
```

Mitigation: ATOMIC.TCP Regular Expression Denial of Service Vulnerability

Transit Access Control Lists (tACLs)

In order to mitigate the effects of the ATOMIC.TCP Regular Expression DoS vulnerability on the IOS IPS device, Transit Access Control Lists (tACLs) can be used on devices that filter traffic destined for IOS IPS inspection by the vulnerable IOS IPS device. Since this vulnerability is exploited by triggering IOS IPS Signature 3123.0 (NetBus Pro Traffic) and this signature looks for traffic on TCP/20034, it is possible to use tACLs to filter on traffic destined for internal address space on TCP/20034.

Note: NetBus Pro runs by default on TCP port 20034, but can be configured to run on other ports.

For more information on tACLs, refer to [Transit Access Control Lists: Filtering at Your Edge](#).

The following tACL denies all TCP packets using TCP destination port 20034 sent to the internal network 192.168.1.0/24. The ACL is applied to traffic destined outbound to VLAN 20.

```
!

!-- Deny connections on TCP port 20034 sent to internal address space (192.168.1.0/24).

!
ip access-list extended atomic-tcp
 deny   tcp any 192.168.1.0 0.0.0.255 eq 20034
 permit ip any 192.168.1.0 0.0.0.255
!

!-- Permit/Deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations.

!

!-- Apply tACL to VLAN interface in the outbound direction.

!
interface Vlan20
```

```
ip address 192.168.1.2 255.255.255.0
ip access-group atomic-tcp out
```

!

Identification: ATOMIC.TCP Regular Expression Denial of Service Vulnerability

Transit Access Control Lists (tACLs)

The `show access-list [ACL name]` command can be used to display output indicating which entries in the ACL have denied packets. The following example indicates that the ACL dropped **6 TCP/20034 packets** that were destined to the 192.168.1.0/24 network.

```
cat6k-01#show access-list atomic-tcp

Extended IP access list atomic-tcp
 10 deny tcp any 192.168.1.0 0.0.0.255 eq 20034 (6 matches)
 20 permit ip any 192.168.1.0 0.0.0.255
cat6K-01#
```

Additional Information

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.

Revision History

Revision 1.0	2007-February-13	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>.

Related Information

- [Access Control Lists and IP Fragments](#)
- [FWSM 3.1 Syslog Messages](#)
- [ASA 7.2 Syslog Messages](#)
- [Static NAT](#)
- [Static Identity NAT](#)
- [Using Modular Policy Framework](#)
- [IPS Signature 3123.0 – NetBus Pro Traffic](#) ([registered](#) customers only)
- [Intercepting and Responding to Network Attacks](#)

