

Cisco Applied Mitigation Bulletin: Detecting and Mitigating Exploitation of the Crafted TCP Packet Denial of Service Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20070124-crafted-tcp.shtml>

Revision 1.0

For Public Release 2007 January 24 1600 UTC (GMT)

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

Contents

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

Cisco Response

Vulnerability Characteristics

This vulnerability can be exploited remotely with no authentication and no user interaction is necessary. If exploited, the attacker may cause a Denial of Service (DoS). The attack vector is through a crafted TCP packet. This vulnerability is not covered by a CVE ID.

This document contains information to assist Cisco customers in mitigating attempts to exploit the Crafted TCP packet vulnerability. Vulnerable, non-affected and fixed software information is available in the PSIRT Security Advisory at <http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml>.

Mitigation Technique Overview

Cisco devices provide several countermeasures for the Crafted TCP packet Denial of Service vulnerability. The most preventive control is provided by applying receive access control lists (rACLs) or by using Control Plane Policing (CoPP) directly on affected devices as this will limit all attack vectors. Receive ACLs (rACLs) are only available on distributed platforms. Details on

workarounds and mitigations that can be applied directly to the affected devices are in the PSIRT advisory at <http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml>. Cisco IOS routers and Cisco PIX, ASA, and Firewall Services Module firewalls can provide effective preventive controls at the network level using access control lists (ACLs). Rapid, active exploitation may resemble a TCP flood. Devices or techniques that prevent or minimize flooding can provide mitigation in addition to ACLs. Although this will not prevent a "low and slow" attack, it will force an attacker to use less effective methods. Detective controls can be performed through syslog messages and access control list **show** commands.

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 Routers



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.

Mitigation: Infrastructure Access Control Lists (iACLs)

Infrastructure ACLs (iACLs) can be used as an effective mitigation technique for the Crafted TCP transit enforcement points. Ideally, mitigation should be performed as close to the target endpoint as possible to provide maximum exposure reduction, while defense in depth could be provided by an additional layer of access control enforced on network edges. The following example should be included in the network infrastructure deny section of an ingress ACL for a router.

In this example, the address block 192.168.131.0/24 is infrastructure address space, while the address block 192.0.2.0/24 is the management network and requires management access to devices via the SSH protocol. Care should be taken to allow required traffic for routing or administrative access prior to denying all infrastructure directed traffic.

Added access list entries should be implemented as part of an infrastructure ACL that filters traffic at network ingress points.

For more information on infrastructure ACLs, refer to [Protecting Your Core: Infrastructure Protection Access Control Lists](#).

```
!-- Network Routing and Administrative traffic  
!-- permitted to infrastructure devices
```

```
access-list 150 permit tcp 192.0.2.0 0.0.0.255 gt 1024 192.168.131.0 0.0.0.2
```

```
!-- Permit additional Layer 3 and Layer 4 traffic destined for infrastruc  
!-- address space as dictated by existing security policies and configuratio
```

```

!-- Permit/deny to infrastructure IP addresses in accordance with security p
!-- Vulnerability-specific deny

access-list 150 deny tcp any 192.168.131.0 0.0.0.255

!-- Default deny to infrastructure IP addresses

access-list 150 deny ip any 192.168.131.0 0.0.0.255

interface GigabitEthernet 0/0
ip access-group 150 in

```

Mitigation: Anti-Spoofing uRPF

This vulnerability can be exploited through the spoofing of IP addresses. Anti-spoof protection in the form of unicast Reverse Path Forwarding (uRPF) can provide limited mitigation if properly configured. This feature should not be relied upon to provide 100% mitigation since spoofed packets may still enter the network from the interface expected by uRPF or allowed by anti-spoofing access-lists. Also care must be taken to ensure that the appropriate uRPF mode (loose or strict) is configured to ensure that legitimate packets are not dropped. Additional information about unicast Reverse Path Forwarding is available at

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_urpf.html.

Identification: Infrastructure Access Control Lists (iACLs)

After the interface ACL is applied to the ingress interface, the command **show access-list *acl number*** can be used to identify the number of packets being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. The following is an example of output for the **show access-list 150** command configured inbound on interface gigabitEthernet 0/0.

```

Extended IP access list 150
 10 permit tcp 192.0.2.0 0.0.0.255 gt 1024 192.168.131.0 0.0.0.255 eq 22
 20 deny tcp any 192.168.131.0 0.0.0.255 (13 matches)
 30 deny ip any 192.168.131.0 0.0.0.255

```

In the above example, 13 TCP packets have been dropped by the ACL configured ingress from the network edge.

Cisco ASA, PIX, and FWSM Firewalls



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.

Mitigation: Transit Access Control Lists (tACLs)

Transit ACLs (tACLs) can be used as an effective mitigation technique for the Crafted TCP packet Denial of Service vulnerability. tACLs will provide effective mitigation from attacks that transit enforcement points. Ideally, mitigation should be performed as close to the target endpoint as possible to provide maximum exposure reduction.

In the following example, the address block 192.168.131.0/24 is infrastructure address space, while the address block 192.0.2.0/24 is the management network and requires management access to devices via the SSH protocol. Care should be taken to allow required traffic for routing or administrative access prior to denying all infrastructure directed traffic.

For more information on transit ACLs, refer to

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml.

```
!-- Network Infrastructure Traffic permitted from untrusted network
!-- (Routing / Administrative Access).

access-list TRANSIT extended permit tcp 192.0.2.0 255.255.255.0 192.168.131.

!-- Network Infrastructure Deny

access-list TRANSIT extended deny tcp any 192.168.131.0 255.255.255.0

!-- Permit/deny in accordance with security policy

access-group TRANSIT in interface outside
```

Mitigation: Anti-Spoofing and Embryonic Connection Limiting with TCP-Intercept

This vulnerability can be exploited through the spoofing of IP addresses. TCP-Intercept provides a more granular level of anti-spoofing protection than that of uRFP for TCP packets. TCP-Intercept will force connecting source endpoints to validate themselves through the use of Syn-cookies. This form of protection can be configured through the use of static network address translation (NAT) or static identity NAT for ASA, PIX, and FWSM Firewalls. In addition, the ASA firewall may be configured through the use of the Modular Policy Framework (MPF). All examples will be covered here.

Additional information on Static NAT is available at

http://www.cisco.com/en/US/docs/security/fwsm/fwsm31/configuration/guide/cfgnat_f.html#wp1043

Additional information on Static Identity NAT is available at

http://www.cisco.com/en/US/docs/security/fwsm/fwsm31/configuration/guide/cfgnat_f.html#wp1043

Additional information on using the Modular Policy Framework to validate TCP connection attempts is available at

<http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/ids.html#wp1042664>.

Static NAT

Static NAT creates a static IP-to-IP mapping performing IP address translation. Static NAT configuration capabilities allow setting embryonic connection and maximum connection limits. In the following example, an embryonic connection limit of one will be set, which will in effect, force all TCP connections to be validated using SYN Cookies once the embryonic connection threshold is reached. In other words, all TCP connections destined for the IP address/network configured in the **static** command below will result in the use of SYN Cookies. The following command will statically map the inside IP address 192.168.131.10 to the outside IP address 192.0.2.10 and will create an embryonic connection limit of 1. Setting embryonic limits to 0 will disable the feature. This

command is available on ASA, PIX and FWSM firewalls.

```
(config)#static (inside,outside) 192.0.2.10 192.168.131.10 tcp 0 1
```

Static Identity NAT

Static Identity NAT creates a static IP-to-IP mapping without performing IP address translation. The benefit of using Static Identity NAT is the ability to set embryonic connection and maximum connection limits as if static IP address translations were taking place. In the following example, an embryonic connection limit of one will be set, which will, in effect, force all TCP connections to be validated using SYN Cookies once the embryonic connection threshold is reached. In other words, all TCP connections destined for the IP address/network configured in the static command below will result in the use of SYN Cookies. The following command will statically map the entire 192.168.131.0/24 subnet and will create an embryonic connection limit of 1. Setting embryonic limits to 0 will disable the feature. This command is available on ASA, PIX, and FWSM firewalls.

```
(config)#static (inside,outside) 192.168.131.0 192.168.131.0 netmask 255.255
```

Modular Policy Framework

TCP-Intercept can also be implemented using the Modular Policy Framework (MPF). TCP-Intercept using MPF is only available on the ASA Firewall. In the following example, an embryonic connection limit of one will be set, which will, in effect, force all TCP connections to be validated using SYN Cookies. The following commands will statically map the entire 192.168.131.0/24 subnet and create an embryonic connection limit of 1. It is possible, using the MPF configuration method, to set an embryonic connection timeout. The default is 30 seconds. In the following example, the policy is being applied to the least trusted interface. Depending on network topologies, however, customers may choose to enforce this policy on other interfaces.

```
(config)#access-list management extended permit tcp any 192.168.131.0 255.25
(config)#class-map connection-limit
(config-cmap)#match access-list management
(config-cmap)#exit
(config)#policy-map spoof-protect
(config-pmap)#class connection-limit
(config-pmap-c)#set connection embryonic-conn-max 1
(config-pmap-c)#exit
(config)#service-policy spoof-protect interface outside
```

Mitigation: Anti-Spoofing uRPF

This vulnerability can be exploited through the spoofing of IP addresses. Anti-spoof protection in the form of unicast Reverse Path Forwarding (uRPF) can provide limited mitigation if properly configured. This feature should not be relied upon to provide 100% mitigation since spoofed packets may still enter the network from the interface expected by uRPF or allowed by anti-spoofing access lists. Also, care must be taken to ensure that the appropriate uRPF mode (loose or strict) is configured to ensure that legitimate packets are not dropped. Additional information about unicast Reverse Path Forwarding is available at

<http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/ids.html#wp1042664>.

Identification: Transit Access Control Lists (tACLs)

After the transit ACL is applied to the ingress interface, the command **show access-list acl number** can be used to identify the number of packets being filtered. The following is an example of output for the **show access-list TRANSIT** command configured inbound on interface outside.

```
R4-ASA5520a#show access-list TRANSIT
access-list TRANSIT; 2 elements
access-list TRANSIT line 1 extended permit tcp
 192.0.2.0 255.255.255.0 192.168.131.0 255.255.255.0 eq ssh (hitcnt=0) 0xf9
access-list TRANSIT line 2 extended deny tcp any
 192.168.131.0 255.255.255.0 (hitcnt=12) 0x2d4bac69
```

In the above example, 12 TCP packets have been dropped by the ACL configured ingress on the firewall. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. In this instance, syslog message 106023 can provide additional context such as source IP address to aid in investigation.

Identification: Syslog Messages

In access lists where no logging keyword was added to the ACL, syslog message 106023 will be generated. For more information on the specific message, refer to [Cisco Security Appliance System Log Message 106023](#).

Information on configuring syslog for the ASA Firewall appliance is available in [Configuring Logging on the Security Appliance](#).

In the following example, the **show logging | grep message** command is used to see more details on denied entries. It is possible to mutate the **grep** command in several ways to provide specific data (for instance, the name of the access list could be used instead or the word Deny). Viewing the specific logging entries, we see the source IP as 192.168.208.63 and a source port of 32886. Using **grep** with the source IP along with the **show logging** command will yield more information, as shown in the second example.

```
R4-ASA5520a(config)#show logging | grep 106023
Jan 10 2007 12:09:25: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/22 by access-group "TRANSIT" [0x77d707a8, 0x0]
Jan 10 2007 12:09:26: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/22 by access-group "TRANSIT" [0x77d707a8, 0x0]
Jan 10 2007 12:09:28: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/22 by access-group "TRANSIT" [0x77d707a8, 0x0]
Jan 10 2007 12:09:32: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/22 by access-group "TRANSIT" [0x77d707a8, 0x0]

R4-ASA5520a(config)#show logging | grep 192.168.208.63
Jan 10 2007 12:09:25: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/22 by access-group "TRANSIT" [0x77d707a8, 0x0]
Jan 10 2007 12:09:26: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/22 by access-group "TRANSIT" [0x77d707a8, 0x0]
Jan 10 2007 12:09:28: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/22 by access-group "TRANSIT" [0x77d707a8, 0x0]
Jan 10 2007 12:09:32: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/22 by access-group "TRANSIT" [0x77d707a8, 0x0]
Jan 10 2007 12:09:40: %ASA-4-106023: Deny tcp src outside:192.168.208.63/328
dst inside:192.168.131.10/22 by access-group "TRANSIT" [0x77d707a8, 0x0]
Jan 10 2007 12:10:20: %ASA-6-302013: Built inbound TCP connection 279830 for
192.168.208.63/32887 (192.168.208.63/32887) to inside:192.168.131.10/110 (
Jan 10 2007 12:10:50: %ASA-6-302014: Teardown TCP connection 279830 for outs
192.168.208.63/32887 to inside:192.168.131.10/110 duration 0:00:30 bytes 0
```

In some instances the ACL may be constructed using the **log** keyword. This will cause a different logging message to be created. For more information on this specific message refer to [Cisco Security Appliance System Log Message 106100](#). Further investigation would follow the same path as the previous example.

```
R4-ASA5520a(config)#show logging | grep 106100
Jan 10 2007 12:27:00: %ASA-6-106100: access-list TRANSIT denied tcp outside/
-> inside/192.168.131.10(22) hit-cnt 1 first hit [0xc0c7f701, 0x0]
Jan 10 2007 12:29:03: %ASA-6-106100: access-list TRANSIT denied tcp outside/
-> inside/192.168.131.10(22) hit-cnt 1 first hit [0xc0c7f701, 0x0]
```

The following syslog messages are associated with the Embryonic limit set through MPF or NAT being exceeded.

- [Cisco Security Appliance System Log Message 201003](#)
- [Cisco Security Appliance System Log Message 201002](#)
- [Cisco Security Appliance System Log Message 407002](#)
- [Cisco Security Appliance System Log Message 201010](#)

For more information, please refer to http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ft_ipacl.html.

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-January-24	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>.

Help us help you.

-
- **Please rate this document.**
- Excellent
- Good
- Average
- Fair
- Poor
-

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)