

Cisco Security Advisory: Multiple Vulnerabilities in Cisco ASA 5500 Series Adaptive Security Appliances

Advisory ID: cisco-sa-20100217-asa

<http://www.cisco.com/warp/public/707/cisco-sa-20100217-asa.shtml>

Revision 1.1

Last Updated 2010 February 17 2150 UTC (GMT)

For Public Release 2010 February 17 1600 UTC (GMT)

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

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)

[Distribution](#)

Summary

Cisco ASA 5500 Series Adaptive Security Appliances are affected by the following vulnerabilities:

- TCP Connection Exhaustion Denial of Service Vulnerability
- Session Initiation Protocol (SIP) Inspection Denial of Service Vulnerabilities
- Skinny Client Control Protocol (SCCP) Inspection Denial of Service Vulnerability
- WebVPN Datagram Transport Layer Security (DTLS) Denial of Service Vulnerability
- Crafted TCP Segment Denial of Service Vulnerability
- Crafted Internet Key Exchange (IKE) Message Denial of Service Vulnerability
- NT LAN Manager version 1 (NTLMv1) Authentication Bypass Vulnerability

These vulnerabilities are not interdependent; a release that is affected by one vulnerability is not necessarily affected by the others.

There are workarounds for some of the vulnerabilities disclosed in this advisory.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100217-asa.shtml>.

[\[Expand all sections\]](#)

[\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

Cisco ASA 5500 Series Adaptive Security Appliances are affected by multiple vulnerabilities. Affected versions of Cisco ASA Software vary depending on the specific vulnerability. For specific version information, refer to the [Software Versions and Fixes](#) section of this advisory.

TCP Connection Exhaustion Denial of Service Vulnerability

Cisco ASA 5500 Series Adaptive Security Appliances may experience a TCP connection

exhaustion condition (no new TCP connections are accepted) that can be triggered through the receipt of specific TCP segments during the TCP connection termination phase. Appliances that are running versions 7.1.x, 7.2.x, 8.0.x, 8.1.x, and 8.2.x are affected when they are configured for any of the following features:

- SSL VPNs
- Cisco Adaptive Security Device Manager (ASDM) Administrative Access
- Telnet Access
- SSH Access
- Virtual Telnet
- Virtual HTTP
- Transport Layer Security (TLS) Proxy for Encrypted Voice Inspection

SIP Inspection Denial of Service Vulnerabilities

Two denial of service (DoS) vulnerabilities affect the SIP inspection feature of Cisco ASA 5500 Series Adaptive Security Appliances. Versions 7.0.x, 7.1.x, 7.2.x, 8.0.x, 8.1.x, and 8.2.x are affected. SIP inspection is enabled by default.

To check if SIP inspection is enabled, issue the **show service-policy | include sip** command and confirm that some output is returned. Sample output is displayed in the following example:

```
ciscoasa#show service-policy | include sip
Inspect: sip , packet 0, drop 0, reset-drop 0
```

Alternatively, an appliance that has SIP inspection enabled has a configuration similar to the following:

```
class-map inspection_default
  match default-inspection-traffic
!
policy-map global_policy
  class inspection_default
    ...
    inspect sip
    ...
!
service-policy global_policy global
```

SCCP Inspection Denial of Service Vulnerability

A denial of service vulnerability affects the SCCP inspection feature of the Cisco ASA 5500

Series Adaptive Security Appliances. Versions 8.0.x, 8.1.x, and 8.2.x are affected. SCCP inspection is enabled by default.

To check if SCCP inspection is enabled, issue the **show service-policy | include skinny** command and confirm that some output is returned. Sample output is displayed in the following example:

```
ciscoasa#show service-policy | include skinny
Inspect: skinny , packet 0, drop 0, reset-drop 0
```

Alternatively, an appliance that has SCCP inspection enabled has a configuration similar to the following:

```
class-map inspection_default
  match default-inspection-traffic
!
policy-map global_policy
  class inspection_default
    ...
    inspect skinny
    ...
!
service-policy global_policy global
```

WebVPN DTLS Denial of Service Vulnerability

Cisco ASA 5500 Series Adaptive Security Appliances are affected by a denial of service vulnerability that exists when WebVPN and DTLS are enabled. Affected versions include 7.1.x, 7.2.x, 8.0.x, 8.1.x, and 8.2.x. Administrators can enable WebVPN with the **enable <interface name>** command in "webvpn" configuration mode. DTLS can be enabled by issuing the **svc dtls enable** command in "group policy webvpn" configuration mode. The following configuration snippet provides an example of a WebVPN configuration that enables DTLS:

```
webvpn
  enable outside
  svc enable
  ...
!
group-policy <group name> internal
group-policy <group name> attributes
  ...
webvpn
```

```
svc dtls enable
...
```

Although WebVPN is disabled by default, DTLS is enabled by default in recent software releases.

Crafted TCP Segment Denial of Service Vulnerability

Cisco ASA 5500 Series Adaptive Security Appliances are affected by a denial of service vulnerability that can be triggered by a malformed TCP segment that transits the appliance. This vulnerability only affects configurations that use the *nailed* option at the end of their **static** statement. Additionally, traffic that matches **static** statement must also be inspected by a Cisco AIP-SSM (an Intrusion Prevention System (IPS) module) in inline mode. IPS inline operation mode is enabled by using the **ips inline {fail-close | fail-open}** command in "class" configuration mode. Cisco ASA 5500 Series Adaptive Security Appliances that are running software versions 7.0.x, 7.1.x, 7.2.x, 8.0.x, 8.1.x, and 8.2.x are affected.

Crafted IKE Message Denial of Service Vulnerability

A crafted IKE message that is sent through an IPsec tunnel that terminates on a Cisco ASA 5500 Series Adaptive Security Appliance could cause all IPsec tunnels that terminate on the same device to be torn down. Versions 7.0.x, 7.1.x, 7.2.x, 8.0.x, 8.1.x, and 8.2.x are affected. IKE is not enabled by default. If IKE is enabled, the **isakmp enable <interface name>** command appears in the configuration.

NTLMv1 Authentication Bypass Vulnerability

An authentication bypass vulnerability affects Cisco ASA 5500 Series Adaptive Security Appliances when NTLMv1 authentication is configured. Versions 7.0.x, 7.1.x, 7.2.x, 8.0.x, 8.1.x, and 8.2.x are affected. Administrators can configure NTLMv1 authentication by defining an Authentication, Authorization, and Accounting (AAA) server group that uses the NTLMv1 protocol with the **aaa-server <AAA server group tag> protocol nt** command and then configuring a service that requires authentication to use that AAA server group. To verify that NTLMv1 authentication is enabled and active, issue the **show aaa-server protocol nt** command. Sample output is displayed in the following example:

```
ciscoasa#show aaa-server protocol nt
Server Group:      test
Server Protocol:  nt
Server Address:   192.168.10.11
Server port:      139
Server status:    ACTIVE, Last transaction (success) at
11:10:08 UTCÂ    Fri Jan 29
```

<output truncated>

Cisco PIX 500 Series Security Appliance Vulnerability Status

Cisco PIX 500 Series Security Appliances are affected by the following vulnerabilities:

- TCP Connection Exhaustion Denial of Service Vulnerability
- SIP Inspection Denial of Service Vulnerabilities
- SCCP Inspection Denial of Service Vulnerability
- Crafted IKE Message Denial of Service Vulnerability
- NTLMv1 Authentication Bypass Vulnerability

Because the Cisco PIX 500 Series Security Appliances reached End of Software Maintenance Releases on July 28, 2009, no further software releases will be available for the Cisco PIX 500 Series Security Appliances. Cisco PIX 500 Series Security Appliances customers are encouraged to migrate to Cisco ASA 5500 Series Adaptive Security Appliances or to implement any applicable workarounds that are listed in the [Workarounds](#) section of this advisory. Fixed software is available for the Cisco ASA 5500 Series Adaptive Security Appliances. For more information, refer to the End of Life announcement at http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5708/ps5709/ps2030/end_of_life_notice_cisco_pix_525_sec_app.html.

How To Determine The Running Software Version

To determine whether a vulnerable version of Cisco ASA Software is running on an appliance, administrators can issue the **show version** command-line interface (CLI) command. The following example shows a Cisco ASA 5500 Series Adaptive Security Appliance that is running software version 8.0(4):

```
ASA#show version
Cisco Adaptive Security Appliance Software Version 8.0
(4)
Device Manager Version 6.0(1)
<output truncated>
```

Customers who use Cisco ASDM to manage devices can locate the software version in the table that is displayed in the login window or upper-left corner of the Cisco ASDM window.

☐ Products Confirmed Not Vulnerable

The Cisco Firewall Services Module (FWSM) is affected by some of the vulnerabilities in this advisory. A separate Cisco Security Advisory has been published to disclose the vulnerabilities

that affect the FWSM. This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20100217-fwsm.shtml>.

With the exception of the Cisco FWSM, no other Cisco products are currently known to be affected by these vulnerabilities.

[Top of the section](#) [Close Section](#)

☐ Details

The Cisco ASA 5500 Series Adaptive Security Appliance is a modular platform that provides security and VPN services. It offers firewall, intrusion prevention (IPS), anti-X, and VPN services.

Cisco ASA 5500 Series Adaptive Security Appliances are affected by the following vulnerabilities:

TCP Connection Exhaustion Denial of Service Vulnerability

Cisco ASA 5500 Series Adaptive Security Appliances may experience a TCP connection exhaustion condition (no new TCP connections are accepted) when specific TCP segments are received during the TCP connection termination phase.

This vulnerability is triggered only when specific TCP segments are sent to certain TCP-based services that terminate on the affected appliance. Although exploitation of this vulnerability requires a TCP three-way handshake, authentication is not required.

This vulnerability is documented in Cisco bug ID [CSCsz77717](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2010-0149.

SIP Inspection Denial of Service Vulnerabilities

Cisco ASA 5500 Series Adaptive Security Appliances are affected by two denial of service vulnerabilities that may cause an appliance to reload during the processing of SIP messages. Appliances are only vulnerable when SIP inspection is enabled.

Only transit traffic can trigger these vulnerabilities; traffic that is destined to the appliance will not trigger the vulnerabilities.

These vulnerabilities are documented in Cisco bug IDs [CSCsy91157](#) ([registered](#) customers only) , and [CSCtc96018](#) ([registered](#) customers only) , and have been assigned CVE IDs CVE-2010-0150, and CVE-2010-0569 respectively.

SCCP Inspection Denial of Service Vulnerability

Cisco ASA 5500 Series Adaptive Security Appliances are affected by a vulnerability that may cause the appliance to reload during the processing of malformed skinny control message. Appliances are only vulnerable when SCCP inspection is enabled.

Only transit traffic can trigger this vulnerability; traffic that is destined to the appliance will not trigger the vulnerability.

This vulnerability is documented in Cisco bug ID [CSCsz79757](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2010-0151.

WebVPN DTLS Denial of Service Vulnerability

Cisco ASA 5500 Series Adaptive Security Appliances are affected by a vulnerability that may cause the appliance to reload when a malformed DTLS message is sent to the DTLS port (by default UDP port 443). Appliances are only vulnerable when they are configured for WebVPN and DTLS transport.

This vulnerability is only triggered by traffic that is destined to the appliance; transit traffic will not trigger the vulnerability.

This vulnerability is documented in Cisco bug ID [CSCtb64913](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2010-0565.

Crafted TCP Segment Denial of Service Vulnerability

Cisco ASA 5500 Series Adaptive Security Appliances are affected by a vulnerability that may cause an appliance to reload when all of the following conditions are met:

1. A malformed, transit TCP segment is received.
2. The TCP segment matches a static NAT translation that has the "nailed" option configured on it.
3. The TCP segment is also processed by the Cisco AIP-SSM, which is configured for inline mode of operation.

A TCP three-way handshake is not necessary to exploit this vulnerability.

This vulnerability is documented in Cisco bug ID [CSCtb37219](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2010-0566.

Crafted IKE Message Denial of Service Vulnerability

Cisco ASA 5500 Series Adaptive Security Appliances contain a vulnerability that may cause all IPsec tunnels terminating on the appliance to be torn down and prevent new tunnels from being established. The tunnels are not torn down immediately; IPsec traffic will continue to flow until the next rekey, at which time the rekey will fail and the tunnels will be torn down. Both site-to-site and remote access VPN tunnels are affected. The vulnerability is triggered when the appliance processes a malformed IKE message on port UDP 4500 that traverses an existing IPsec tunnel. The only way to recover and re-establish IPsec VPN tunnels is to reload the appliance.

When this vulnerability is exploited, the security appliance will generate syslog messages 713903 and 713906, which will be followed by the loss of IPsec peers.

This vulnerability is documented in Cisco bug ID [CSCtc47782](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2010-0567.

NTLMv1 Authentication Bypass Vulnerability

Cisco ASA 5500 Series Adaptive Security Appliances contain a vulnerability that could result in authentication bypass when the affected appliance is configured to authenticate users against Microsoft Windows servers using the NTLMv1 protocol.

Users can bypass authentication by providing an an invalid, crafted username during an authentication request. Any services that use a AAA server group that is configured to use the NTLMv1 authentication protocol is affected. Affected services include:

- Telnet access to the security appliance
- SSH access to the security appliance
- HTTPS access to the security appliance (including Cisco ASDM access)
- Serial console access
- Privileged (enable) mode access
- Cut-through proxy for network access
- VPN access

This vulnerability is documented in Cisco bug ID [CSCte21953](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2010-0568.

[Top of the section](#) [Close Section](#)

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

TCP Connection Exhaustion Denial of Service Vulnerability

CSCsz77717 -- TCP sessions remain in CLOSEWAIT indefinitely					
Calculate the environmental score of CSCsz77717					
CVSS Base Score - 7.1					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	None	Complete
CVSS Temporal Score - 5.9					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

SIP Inspection Denial of Service Vulnerabilities

CSCsy91157 -- Watchdog when inspecting malformed SIP traffic

Calculate the environmental score of [CSCsy91157](#)

CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - **6.4**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCtc96018 -- ASA watchdog when inspecting malformed SIP traffic

Calculate the environmental score of [CSCtc96018](#)

CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - **6.4**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

SCCP Inspection Denial of Service Vulnerability

CSCsz79757 -- Traceback - Thread Name: Dispatch Unit with skinny inspect enabled

Calculate the environmental score of [CSCsz79757](#)

CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

WebVPN DTLS Denial of Service Vulnerability

CSCtb64913 -- WEBVPN: page fault in thread name dispatch unit, eip udpmod_user_put					
Calculate the environmental score of CSCtb64913					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

Crafted TCP Segment Denial of Service Vulnerability

CSCtb37219 -- Traceback in Dispatch Unit AIP-SSM Inline and nailed option on static					
Calculate the environmental score of CSCtb37219					
CVSS Base Score - 7.1					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact

Network	Medium	None	None	None	Complete
CVSS Temporal Score - 5.9					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

Crafted IKE Message Denial of Service Vulnerability

CSCtc47782 -- Malformed IKE traffic causes rekey to fail					
Calculate the environmental score of CSCtc47782					
CVSS Base Score - 5.0					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Partial
CVSS Temporal Score - 4.1					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

NTLMv1 Authentication Bypass Vulnerability

CSCte21953 -- ASA may allow authentication of an invalid username for NT auth					
Calculate the environmental score of CSCte21953					
CVSS Base Score - 7.1					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Complete	None	None
CVSS Temporal Score - 6.2					
Exploitability		Remediation Level		Report Confidence	

High	Official-Fix	Confirmed
------	--------------	-----------

[Top of the section](#) [Close Section](#)

☐ Impact

TCP Connection Exhaustion Denial of Service Vulnerability

Successful exploitation of this vulnerability may lead to an exhaustion condition where the affected appliance cannot accept new TCP connections. A reload of the appliance is necessary to recover from the TCP connection exhaustion condition. If a TCP-based protocol is used for device management (like telnet, SSH, or HTTPS), a serial console connection may be needed to access to the appliance.

SIP Inspection Denial of Service Vulnerabilities

Successful exploitation of this vulnerability may cause a reload of the affected appliance. Repeated exploitation could result in a sustained DoS condition.

SCCP Inspection Denial of Service Vulnerability

Successful exploitation of this vulnerability may cause a reload of the affected appliance. Repeated exploitation could result in a sustained DoS condition.

WebVPN DTLS Denial of Service Vulnerability

Successful exploitation of this vulnerability may cause a reload of the affected appliance. Repeated exploitation could result in a sustained DoS condition.

Crafted TCP Segment Denial of Service Vulnerability

Successful exploitation of this vulnerability may cause a reload of the affected appliance. Repeated exploitation could result in a sustained DoS condition.

Crafted IKE Message Denial of Service Vulnerability

Successful exploitation of this vulnerability could cause all IPsec VPN tunnels (LAN-to-LAN or remote) that terminate on the security appliance to be torn down and prevent new tunnels from being established. A manual reload of the appliance is required to re-establish all VPN tunnels.

NTLMv1 Authentication Bypass Vulnerability

Successful exploitation of this vulnerability could result in unauthorized access to the network or appliance.

[Top of the section](#) [Close Section](#)

☐ 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.

The following table contains the first fixed software release of each vulnerability. A device running a version of the given release in a specific row (less than the First Fixed Release) is known to be vulnerable.

Vulnerability	Major Release	First Fixed Release
TCP Connection Exhaustion Denial of Service Vulnerability (CSCsz77717)	7.0	Not affected
	7.2	7.2(4.46)
	8.0	8.0(4.38)
	8.1	8.1(2.29)
	8.2	8.2(1.5)
SIP Inspection Denial of Service Vulnerabilities (CSCsy91157 and CSCtc96018)	7.0	7.0(8.10)
	7.2	7.2(4.45)
	8.0	8.0(5.2)
	8.1	8.1(2.37)
	8.2	8.2(1.16)

SCCP Inspection Denial of Service Vulnerability (CSCsz79757)	7.0	Not affected
	7.2	Not affected
	8.0	8.0(4.38)
	8.1	8.1(2.29)
	8.2	8.2(1.2)
WebVPN DTLS Denial of Service Vulnerability (CSCtb64913)	7.0	Not affected
	7.2	7.2(4.45)
	8.0	8.0(4.44)
	8.1	8.1(2.35)
	8.2	8.2(1.10)
Crafted TCP Segment Denial of Service Vulnerability (CSCtb37219)	7.0	7.0(8.10)
	7.2	7.2(4.45)
	8.0	8.0(4.44)
	8.1	8.1(2.35)
	8.2	8.2(1.10)
Crafted IKE Message Denial of Service Vulnerability (CSCtc47782)	7.0	7.0(8.10)
	7.2	7.2(4.45)
	8.0	8.0(5.1)
	8.1	8.1(2.37)
	8.2	8.2(1.15)
NTLMv1 Authentication Bypass Vulnerability (CSCte21953)	7.0	7.0(8.10)
	7.2	7.2(4.45)
	8.0	8.0(5.7)
	8.1	8.1(2.40), available early March 2010
	8.2	8.2(2.1)

Note: Cisco ASA Software versions 7.1.x are affected by some of the vulnerabilities in this

advisory. However, no fixed 7.1.x software versions are planned because the 7.1.x major release has reached the End of Software Maintenance Releases milestone. Refer to the [EOL/EOS for the Cisco ASA 5500 Series Adaptive Security Appliance Software v7.1](#) notice for further information.

Fixed Cisco ASA Software can be downloaded from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ASAPSIRT?psrtdcat20e2>

Recommended Releases

Releases 7.0(8.10), 7.2(4.46), 8.0(5.9), 8.1(2.40) (available early March 2010), and 8.2(2.4) are recommended releases because they contain the fixes for all vulnerabilities in this advisory. Cisco recommends upgrading to a release that is equal to or later than these recommended releases.

[Top of the section](#) [Close Section](#)

Workarounds

In addition to the recommendations described below, mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory: <http://www.cisco.com/warp/public/707/cisco-amb-20100217-asa.shtml>

TCP Connection Exhaustion Denial of Service Vulnerability

It is possible to mitigate this vulnerability for TCP-based services that are offered to known clients. For example, it may be possible to restrict SSH, Cisco ASDM/HTTPS, and Telnet administrative access to known hosts or IP subnetworks. For other services like remote access SSL VPN, where clients connect from unknown hosts and networks, no mitigations exist.

SIP Inspection Denial of Service Vulnerabilities

These vulnerabilities can be mitigated by disabling SIP inspection if it is not required. Administrators can disable SIP inspection by issuing the **no inspect sip** command in class configuration sub-mode within policy-map configuration.

SCCP Inspection Denial of Service Vulnerability

This vulnerability can be mitigated by disabling SCCP inspection if it is not required. Administrators can disable SCCP inspection by issuing the **no inspect skinny** command in class configuration sub-mode within the policy-map configuration.

WebVPN DTLS Denial of Service Vulnerability

This vulnerability can be mitigated by disabling DTLS transport for WebVPN. Administrators can disable DTLS by issuing the **no svc dtls enable** command under the "webvpn" attributes section of the corresponding group policy.

Crafted TCP Segment Denial of Service Vulnerability

Possible workarounds for this vulnerability are the following:

- Migrate from "nailed" static NAT entries to TCP-state bypass.
- Use the Cisco AIP-SSM in promiscuous mode. This mode can be configured by issuing the **ips promiscuous** command in "class" configuration mode.
- Disable IPS inspection for "nailed" static NAT entries.
- If possible, change "nailed" static NAT entries to standard static NAT entries.

Crafted IKE Message Denial of Service Vulnerability

A workaround for this vulnerability is to prevent UDP port 4500 traffic from ever traversing IPsec tunnels terminating on the Cisco ASA 5500 Series Adaptive Security Appliance. This may be feasible since in most cases there is no need for allowing IPsec tunnels inside IPsec tunnels. Filtering out UDP port 4500 traffic across an IPsec tunnel can be accomplished by using a VPN filter, as shown in the following example:

```
!-- Deny only UDP port 4500 traffic and allow everything else
```

```
access-list VPNFILTER extended deny udp any any eq 4500  
access-list VPNFILTER extended permit ip any any
```

```
!-- Create a group policy and specify a VPN filter that uses the
```

```
!-- previous ACL
```

```
group-policy VPNPOL internal  
group-policy VPNPOL attributes  
  vpn-filter value VPNFILTER
```

```
!-- Reference the group policy with the VPN filter from
```

the tunnel group

```
tunnel-group 172.16.0.1 type ipsec-l2l  
tunnel-group 172.16.0.1 general-attributes  
default-group-policy VPNPOL
```

For this workaround to be effective, the group policy needs to be applied to all site-to-site (tunnel type "ipsec-l2l") and remote access (tunnel type "ipsec-ra") tunnel groups.



Warning: In addition to filtering out IKE traffic on UDP port 4500, this workaround may also affect other protocols like DNS and SNMP that send traffic on UDP port 4500. For example, if a DNS resolver sends traffic from UDP port 4500 to a DNS server, the response from the DNS server will be destined to UDP port 4500, which then may be filtered out by the filter used in this workaround.

For a more comprehensive example of the VPN filter feature of the Cisco ASA 5500 Series Adaptive Security Appliances, refer to the whitepaper "PIX/ASA 7.x and Later: VPN Filter (Permit Specific Port or Protocol) Configuration Example for L2L and Remote Access" available at:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00808c9a87.shtml

In addition, if the security appliance does not terminate any tunnels, the vulnerability can be mitigated by disabling IKE by issuing the **no isakmp enable** *<interface name>* command.

NTLMv1 Authentication Bypass Vulnerability

If NTLMv1 authentication is required, there are no workarounds for this vulnerability. If NTLMv1 authentication can be substituted by other authentication protocols (LDAP, RADIUS, TACACS+, etc.), it is possible to mitigate the vulnerability.

[Top of the section](#) [Close Section](#)

☐ Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. 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/en/US/docs/general/warranty/English/EU1KEN_.html, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract

customers must be requested through the TAC.

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any public announcements or malicious use of any of the vulnerabilities described in this advisory.

TCP Connection Exhaustion Denial of Service Vulnerability

This vulnerability was discovered during the resolution of a customer service request.

SIP Inspection Denial of Service Vulnerabilities

[CSCsy91157](#) ([registered](#) customers only) was discovered during internal testing. [CSCtc96018](#) ([registered](#) customers only) was discovered during the resolution of customer service requests.

SCCP Inspection Denial of Service Vulnerability

This vulnerability was discovered during the resolution of customer service requests.

WebVPN DTLS Denial of Service Vulnerability

This vulnerability was discovered during the resolution of customer service requests.

Crafted TCP Segment Denial of Service Vulnerability

This vulnerability was discovered during internal testing.

Crafted IKE Message Denial of Service Vulnerability

This vulnerability was discovered during the resolution of customer service requests.

NTLMv1 Authentication Bypass Vulnerability

This vulnerability was discovered during internal testing.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20100217-asa.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

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 1.1	2010-February-17	Added link to Applied Mitigation Bulletin.
Revision 1.0	2010-February-17	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](#)

© 2009 - 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

[Trademarks of Cisco Systems, Inc.](#)