

Cisco Security Advisory: Remote Access VPN and SIP Vulnerabilities in Cisco PIX and Cisco ASA

Advisory ID: cisco-sa-20080903-asa

<http://www.cisco.com/warp/public/707/cisco-sa-20080903-asa.shtml>

Revision 1.0

For Public Release 2008 September 3 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](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

Multiple vulnerabilities exist in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances that may result in a reload of the device or disclosure of confidential information. This security advisory outlines details of the following vulnerabilities:

- Erroneous SIP Processing Vulnerabilities
- IPSec Client Authentication Processing Vulnerability
- SSL VPN Memory Leak Vulnerability
- URI Processing Error Vulnerability in SSL VPNs
- Potential Information Disclosure in Clientless VPNs

Note: These vulnerabilities are independent of each other. A device may be affected by one vulnerability and not affected by another. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate some of these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080903-asa.shtml>.

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

☐ Affected Products

The following paragraphs describe the affected Cisco ASA and Cisco PIX software versions:

☐ Vulnerable Products

The following sections provide details on the versions of Cisco ASA that are affected by each vulnerability.

The **show version** command-line interface (CLI) command can be used to determine if a vulnerable version of the Cisco PIX or Cisco ASA software is running. The following example shows a Cisco ASA device that runs software release 8.0(2):

```
ASA# show version
```

```
Cisco Adaptive Security Appliance Software Version 8.0  
(2)
```

Device Manager Version 6.0(1)

[...]

Customers who use the Cisco Adaptive Security Device Manager (ASDM) to manage their devices can find their software version displayed in a table in the login window or in the upper left corner of the ASDM window.

Erroneous SIP Processing Vulnerabilities

Cisco PIX and Cisco ASA devices configured for SIP inspection are vulnerable to multiple processing errors that may result in denial of service attacks. Cisco PIX and ASA software versions prior to 7.0(7)16, 7.1(2)71, 7.2(4)7, 8.0(3)20, and 8.1(1)8 are vulnerable to these SIP processing errors.

IPSec Client Authentication Processing Vulnerability

Cisco PIX and Cisco ASA devices that terminate remote access VPN connections are vulnerable to a denial of service attack if the device is running software versions prior to 7.2(4)2, 8.0(3)14, and 8.1(1)4. Cisco PIX and Cisco ASA devices that run software versions 7.0 and 7.1 are not affected by this vulnerability.

SSL VPN Memory Leak Vulnerability

Cisco ASA devices that terminate clientless remote access VPN connections are vulnerable to a denial of service attack affecting the SSL processing software if the device is running a software version prior to 7.2(4)2, 8.0(3)14, or 8.1(1)4. Cisco ASA devices that run software versions 7.0 and 7.1 are not affected by this vulnerability.

URI Processing Error Vulnerability in SSL VPNs

Cisco ASA devices that terminate clientless remote access VPN connections are vulnerable to a denial of service attack in the HTTP server if the device is running software versions prior to 8.0(3)15, and 8.1(1)5. Cisco ASA devices that run software versions 7.0, 7.1, or 7.2 are not affected by this vulnerability.

Potential Information Disclosure in Clientless VPNs

Cisco ASA devices that terminate clientless remote access VPN connections are vulnerable to potential information disclosure if the device is running affected 8.0 or 8.1 software versions. Cisco ASA devices running software versions 7.0, 7.1, or 7.2 are not affected by this

vulnerability. Cisco ASA devices the run software versions prior to 8.0(3)15 and 8.1(1)4, or after 8.0(3)16 and 8.1(1)5 are also not affected by this vulnerability.

☐ Products Confirmed Not Vulnerable

The Cisco Firewall Services Module (FWSM) is not affected by any of these vulnerabilities. Cisco PIX security appliances running software versions 6.x are not vulnerable. IOS, IOS XR, and Cisco Unified Border Elements (CUBE) are not vulnerable to these issues. No other Cisco products are currently known to be affected by these vulnerabilities.

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

☐ Details

The following sections provide details to help determine if a device may be affected by any of the vulnerabilities.

Erroneous SIP Processing Vulnerabilities

Cisco PIX and Cisco ASA devices configured for SIP inspection are vulnerable to multiple processing errors that may result in denial of service attacks. All Cisco PIX and Cisco ASA software releases may be vulnerable to these SIP processing vulnerabilities. A successful attack may result in a reload of the device.

SIP inspection is enabled with the **inspect sip** command.

To determine whether the Cisco PIX or Cisco ASA security appliance is configured to support inspection of sip packets, log in to the device and issue the CLI command **show service-policy | include sip**. If the output contains the text **Inspect: sip** and some statistics, then the device has a vulnerable configuration. The following example shows a vulnerable Cisco ASA Security Appliance:

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

asa#
```

These vulnerability is documented in the following Cisco Bug IDs and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-2732.

- [CSCsq07867](#) ([registered](#) customers only)
- [CSCsq57091](#) ([registered](#) customers only)
- [CSCsk60581](#) ([registered](#) customers only)
- [CSCsq39315](#) ([registered](#) customers only)

IPSec Client Authentication Processing Vulnerability

Cisco PIX and Cisco ASA devices configured to terminate client based VPN connections are vulnerable to a crafted authentication processing vulnerability if they are running software versions 7.2, 8.0, or 8.1. Devices that run software versions 7.0 or 7.1 are not affected by this vulnerability.

A successful attack may result in a reload of the device.

Remote access VPN connections will have Internet Security Association and Key Management Protocol (ISAKMP) enabled on an interface with the **crypto** command, such as: **crypto isakmp enable outside**.

This vulnerability is documented in Cisco Bug ID [CSCso69942](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-2733.

SSL VPN Memory Leak Vulnerability and URI Processing Error Vulnerability in SSL VPNs

A crafted SSL or HTTP packet may cause a denial of service condition on a Cisco ASA device that is configured to terminate clientless VPN connections. A successful attack may result in a reload of the device.

Cisco ASA devices that run versions 7.2, 8.0, or 8.1 with clientless SSL VPNs enabled may be affected by this vulnerability. Devices that run software versions 7.0 and 7.1 are not affected by this vulnerability.

Clientless VPN, SSL VPN Client, and AnyConnect connections are enabled via the **webvpn** command. For example, the following configuration shows a Cisco ASA with Clientless VPNs configured and enabled. In this case the ASA will listen for VPN connections on the default port, TCP port 443:

```
http server
enable
!
webvpn
enable outside
```

Note that with this particular configuration, the device is vulnerable to attacks coming from the outside interface due to the **enable outside** command within the webvpn group configuration.

These vulnerabilities are documented in Cisco Bug ID [CSCso66472](#) ([registered](#) customers only) and [CSCsq19369](#) ([registered](#) customers only) . They have been assigned Common Vulnerabilities and Exposures (CVE) identifiers CVE-2008-2734 and CVE-2008-2735.

Potential Information Disclosure in Clientless VPNs

On Cisco ASA devices configured to terminate clientless VPN connections, an attacker may be able to discover potentially sensitive information such as usernames and passwords. This attack requires an attacker to convince a user to visit a rogue web server, reply to an e-mail, or interact with a service to successfully exploit the vulnerability.

Cisco ASA devices running software versions 8.0 or 8.1 with clientless VPNs enabled may be affected by this vulnerability. Cisco ASA devices running that run software versions 7.0, 7.1, or 7.2 are not vulnerable to this vulnerability.

Clientless SSL VPN connections are enabled via the **webvpn** command. For example, the following configuration shows a Cisco ASA device with Clientless VPNs configured and enabled. In this case the Cisco ASA device will listen for VPN connections on the default port, TCP port 443:

```
http server
enable
!
webvpn
enable outside
```

Note that with this particular configuration, the device is vulnerable to attacks coming from the outside interface due to the **enable outside** command within the webvpn group configuration.

This vulnerability is documented in Cisco Bug ID [CSCsq45636](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-2736.

[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 calculated 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>.

Erroneous SIP Processing Vulnerabilities

Memory corruption with traceback in SIP inspection code Calculate the environmental score of CSCsq07867					
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	

Memory corruption and traceback when inspecting malformed SIP packets Calculate the environmental score of CSCsq57091					
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	

Device reload possible when SIP inspection is enabled Calculate the environmental score of CSCsk60581					
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	

Traceback when processing malformed SIP requests Calculate the environmental score of CSCsq39315					
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	

IPSec Client Authentication Processing Vulnerability

Traceback in Remote Access Authentication Code Calculate the environmental score of [CSCso69942](#)

CVSS Base Score - **6.8**

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

CVSS Temporal Score - **5.6**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

SSL VPN Memory Leak Vulnerability

Crypto memory leak causing Clientless SSL VPNs to hang Calculate the environmental score of [CSCso66472](#)

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

URI Processing Error Vulnerability in SSL VPNs

URI Processing Error in Clientless SSL VPN connections Calculate the environmental score of [CSCsq19369](#)

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	

Potential Information Disclosure in Clientless VPNs

Potential Information Disclosure in Clientless SSL VPNs Calculate the environmental score of CSCsq45636					
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 - 5.9					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

☐ Impact

Successful exploitation of the Erroneous SIP Processing Vulnerabilities, IPsec Client Authentication Processing Vulnerability, SSL VPN Memory Leak Vulnerability, or URI Processing Error Vulnerability in SSL VPNs may result in the device reloading. This can be repeatedly exploited and may lead to a denial of service attack.

The Potential Information Disclosure in Clientless SSL VPNs vulnerability may allow an attacker to obtain user and group credentials if the user interacts with a rogue system or document.

[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 list contains the first fixed software release of each vulnerability:

Vulnerability	Bug ID	Affected Release	First Fixed Release
Memory corruption with traceback in SIP inspection code	CSCsq07867	7.0	7.0(7)15
		7.1	7.1(2)70
		7.2	Not vulnerable
		8.0	Not vulnerable
		8.1	Not vulnerable
Memory corruption and traceback when inspecting malformed SIP packets	CSCsq57091	7.0	Not vulnerable
		7.1	Not vulnerable
		7.2	7.2(4)7
		8.0	8.0(3)20
		8.1	8.1(1)8
Device reload possible when SIP inspection is enabled	CSCsk60581	7.0	Not vulnerable
		7.1	Not vulnerable
		7.2	7.2(3)18

		8.0	8.0(3)8
		8.1	Not vulnerable
Traceback when processing malformed SIP requests	CSCsq39315	7.0	7.0(7)16
		7.1	7.1(2)71
		7.2	Not vulnerable
		8.0	Not vulnerable
		8.1	Not vulnerable
Traceback in Remote Access Authentication Code	CSCso69942	7.0	Not vulnerable
		7.1	Not vulnerable
		7.2	7.2(4)2
		8.0	8.0(3)14
		8.1	8.1(1)4
Crypto memory leak causing Clientless SSL VPNs to hang	CSCso66472	7.0	Not vulnerable
		7.1	Not vulnerable
		7.2	7.2(4)2
		8.0	8.0(3)14
		8.1	8.1(1)4
HTTP Processing Error in Clientless SSL VPN connections	CSCsq19369	7.0	Not vulnerable
		7.1	Not vulnerable
		7.2	Not vulnerable
		8.0	8.0(3)15

		8.1	8.1(1)5
Potential Information Disclosure in Clientless SSL VPNs	CSCsq45636	7.0	Not vulnerable
		7.1	Not vulnerable
		7.2	Not vulnerable
		8.0	8.0(3)16
		8.1	8.1(1)6
Recommended Release		7.0	7.0(7)16
		7.1	7.1(2)72
		7.2	7.2(4)9
		8.0	8.0(4)
		8.1	8.1(1)8

The "Recommended Release" row indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. A device running a version of the given release in a specific row (less than the First Fixed Release) is known to be vulnerable. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Release" row of the table.

Fixed Cisco PIX software can be downloaded from: <http://www.cisco.com/cgi-bin/tablebuild.pl/pix-interim?psrtdcat20e2>

Fixed Cisco ASA software can be downloaded from: <http://www.cisco.com/cgi-bin/tablebuild.pl/asa-interim?psrtdcat20e2>

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

Workarounds

The following workarounds may help some customers mitigate these vulnerabilities.

Additional 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://>

Erroneous SIP Processing Vulnerabilities

SIP inspection should be disabled if it is not needed and temporarily disabling the feature will mitigate the SIP processing vulnerabilities. SIP inspection can be disabled with the command **no inspect sip**.

IPSec Authentication Processing Vulnerability

Use strong group credentials for remote access VPN connections and do not give out the group credentials to end users.

SSL VPN Memory Leak Vulnerability and URI Processing Error Vulnerability in SSL VPNs

IPSec clients are not vulnerable to this issue and may be used in conjunction with strong group credentials until the device can be upgraded.

Potential Information Disclosure in Clientless SSL VPNs

Client based VPN connections are not vulnerable to the information disclosure vulnerability. If you are running 8.0(3)15, 8.0(3)16, 8.1(1)4, or 8.1(1)5, you may safely use client based VPN connections as an alternative to clientless VPNs.

[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/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

☐ **Exploitation and Public Announcements**

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

These vulnerabilities were reported to Cisco by customers that experienced these issues during normal operation of their equipment and through internal testing efforts.

[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-20080903-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.

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

☐ **Revision History**

Revision 1.0	2008-Sept-03	Initial public release.
--------------	--------------	-------------------------

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

☐ **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>.

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

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](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

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