

Cisco Security Advisory: Multiple Vulnerabilities in Cisco PIX and Cisco ASA

Advisory ID: cisco-sa-20081022-asa

<http://www.cisco.com/warp/public/707/cisco-sa-20081022-asa.shtml>

Revision 1.0

For Public Release 2008 October 22 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. This security advisory outlines details of these vulnerabilities:

- Windows NT Domain Authentication Bypass Vulnerability
- IPv6 Denial of Service Vulnerability
- Crypto Accelerator Memory Leak Vulnerability

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-20081022-asa.shtml>.

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

☐ Affected Products

☐ Vulnerable Products

The following are the details about each vulnerability described within this advisory.

Windows NT Domain Authentication Bypass Vulnerability

Because of a Microsoft Windows NT Domain authentication issue the Cisco ASA and Cisco PIX devices may be susceptible to a VPN authentication bypass vulnerability. Cisco ASA or Cisco PIX security appliances that are configured for IPsec or SSL-based remote access VPN using Microsoft Windows NT Domain authentication may be vulnerable. Devices that are using any other type of external authentication (that is, LDAP, RADIUS, TACACS+, SDI, or local database) are not affected by this vulnerability.

The following example demonstrates how Windows NT domain authentication is configured using the command line interface (CLI) on the Cisco ASA:

```
aaa-server NTAUTH protocol nt
aaa-server NTAUTH (inside) host 10.1.1.4
```

```
nt-auth-domain-controller primary1
```

Alternatively, to see if a device is configured for Windows NT Domain authentication use the **show running-config | include nt-auth-domain-controller** command.

IPv6 Denial of Service Vulnerability

Cisco ASA and Cisco PIX security appliances that are running software version 7.2(4)9 or 7.2(4)10 and configured for IPv6 may be vulnerable. This vulnerability does not affect devices configured only for IPv4.

Note: IPv6 functionality is turned off by default.

IPv6 is enabled on the Cisco ASA and Cisco PIX security appliance using the **ipv6 address** interface command. To verify if a device is configured for IPv6 use the **show running-config | include ipv6** command.

Alternatively, you can display the status of interfaces configured for IPv6 using the **show ipv6 interface** command in privileged EXEC mode, as shown in the following example:

```
hostname# show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
dmz [up/up]
    unassigned
```

In this example, the **outside** and **dmz** interfaces are not configured for IPv6.

Crypto Accelerator Memory Leak Vulnerability

Cisco ASA security appliances may experience a memory leak that can be triggered by a series of crafted packets. This memory leak occurs in the initialization code for the hardware crypto accelerator. Devices that are running software versions in the 8.0.x release are vulnerable.

Note: Cisco ASA appliances that are running software versions in the 7.0, 7.1, and 7.2 releases are not vulnerable. The Cisco PIX security appliance is not affected by this vulnerability.

Determination of Software Versions

The show version command-line interface (CLI) command can be used to determine whether a vulnerable version of the Cisco PIX or Cisco ASA software is running. The following example shows a Cisco ASA Security Appliance that runs software release 8.0(4):

```
ASA# show version

Cisco Adaptive Security Appliance Software Version
8.0(4)
Device Manager Version 6.0(1)

[...]
```

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

☐ Products Confirmed Not Vulnerable

The Cisco Firewall Services Module (FWSM) is not affected by any of these vulnerabilities. Cisco PIX security appliances running versions 6.x are not vulnerable. No other Cisco products are currently known to be affected by these vulnerabilities.

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

☐ Details

This Security Advisory describes multiple distinct vulnerabilities. These vulnerabilities are independent of each other.

Windows NT Domain Authentication Bypass Vulnerability

Because of a Microsoft Windows NT Domain authentication issue the Cisco ASA and Cisco PIX devices may be susceptible to a VPN authentication bypass vulnerability. Cisco ASA or Cisco PIX security appliances configured for IPsec or SSL-based remote access VPN may be vulnerable.

Note: Cisco ASA or Cisco PIX security appliances that are configured for IPsec or SSL-based remote access VPN using any other type of external authentication (that is, LDAP, RADIUS, TACACS+, SDI, or local database) are not affected by this vulnerability.

The Cisco ASA security appliance supports Microsoft Windows server operating systems that

support NTLM version 1, collectively referred to as "NT servers". NT Domain authentication is supported only for remote access VPNs.

This vulnerability is documented in Cisco Bug ID [CSCsu65735](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) identifiers CVE-2008-3815.

IPv6 Denial of Service Vulnerability

A specially crafted IPv6 packet may cause the Cisco ASA and Cisco PIX security appliances to reload. Devices that are running software version 7.2(4)9 or 7.2(4)10 and configured for IPv6 may be vulnerable. This vulnerability does not affect devices that are configured only for IPv4.

Note: Devices that are running software versions in the 7.0, 7.1, 8.0, and 8.1 releases are not vulnerable.

To configure IPv6 on a Cisco ASA or Cisco PIX security appliance, at a minimum, each interface needs to be configured with an IPv6 link-local address. Additionally, you can add a global address to the interface.

Note: Only packets that are destined to the device (not transiting the device) may trigger the effects of this vulnerability. These packets must be destined to an interface configured for IPv6.

This vulnerability is documented in Cisco Bug ID [CSCsu11575](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-3816.

Crypto Accelerator Memory Leak Vulnerability

The Cisco ASA security appliances may experience a memory leak triggered by a series of packets. This memory leak occurs in the initialization code for the hardware crypto accelerator.

Note: Only packets destined to the device (not transiting the device) may trigger this vulnerability.

The following Cisco ASA features use the services the crypto accelerator provides, and therefore may be affected by this vulnerability:

- Clientless WebVPN, SSL VPN Client, and AnyConnect Connections
- ASDM (HTTPS) Management Sessions
- Cut-Through Proxy for Network Access
- TLS Proxy for Encrypted Voice Inspection
- IP Security (IPsec) Remote Access and Site-to-site VPNs
- Secure Shell (SSH) Access

This vulnerability is documented in Cisco Bug ID [CSCsj25896](#) ([registered](#) customers only) and has been assigned the Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-3817.

[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> .

CSCsu65735 - Windows NT Domain Authentication Bypass Vulnerability					
Calculate the environmental score of CSCsu65735					
CVSS Base Score - 4.3					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Partial	None	None
CVSS Temporal Score - 3.7					
Exploitability	Remediation Level		Report Confidence		

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

CSCsu11575 - Cisco ASA may reload after receiving certain IPv6 packets

Calculate the environmental score of [CSCsu11575](#)

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

CSCsj25896 - Crypto Accelerator Memory Leak

Calculate the environmental score of [CSCsj25896](#)

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

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

☐ **Impact**

Successful exploitation of the VPN Authentication Bypass Vulnerability may allow an attacker to successfully connect to the Cisco ASA via remote access IPsec or SSL-based VPN. The Denial of Service (DoS) vulnerabilities may cause a reload of the affected device. Repeated exploitation could

result in a sustained DoS condition.

[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	Affected Release	First Fixed Version
Windows NT Domain Authentication Bypass Vulnerability	7.0	7.0(8)3
	7.1	7.1(2)78
	7.2	7.2(4)16
	8.0	8.0(4)6
	8.1	8.1(1)13
IPv6 Denial of Service Vulnerability	7.0	Not Vulnerable
	7.1	Not Vulnerable
	7.2	7.2(4)11
	8.0	Not Vulnerable
	8.1	Not Vulnerable
Crypto Accelerator Memory Leak Vulnerability	7.0	Not Vulnerable
	7.1	Not Vulnerable
	7.2	Not Vulnerable
	8.0	8.0(4)
	8.1	8.1(2)

The following maintenance software releases are the first software releases that contain the fixes for the vulnerabilities mentioned in this Security Advisory:

Fixed PIX software can be downloaded from:

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

Fix ASA software can be downloaded from:

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

For the "Windows NT Domain Authentication Bypass Vulnerability", only interim fixed software is currently available. Customers wishing to upgrade to a fixed version instead of applying a workaround may download PIX and ASA interim versions from:

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

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

☐ Workarounds

This Security Advisory describes multiple distinct vulnerabilities. These vulnerabilities and their respective workarounds are independent of each other.

Windows NT Domain Authentication Bypass Vulnerability

LDAP authentication is not affected by this vulnerability. As a workaround, you can enable a different type of external authentication for Remote Access VPN instead of Windows NT Domain authentication.

Note: For more information about support for a specific AAA server type, refer to the following link: <http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/aaa.html#wp1069492>

IPv6 Denial of Service Vulnerability

Customers that do not require IPv6 functionality on their devices can use the **no ipv6 address** interface sub-command to disable processing of IPv6 packets and eliminate their exposure

Crypto Accelerator Memory Leak Vulnerability

There are no workarounds for this 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 the vulnerabilities described in this advisory.

These vulnerabilities were found during internal testing and during the resolution of a technical support service request.

[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-20081022-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-October-22	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.](#)