

# Cisco Security Advisory: Cisco PIX and ASA Time-to-Live Vulnerability

Advisory ID: cisco-sa-20080123-asa

<http://www.cisco.com/warp/public/707/cisco-sa-20080123-asa.shtml>

## Revision 1.1

Last Updated 2008 April 25 2000 UTC (GMT)

For Public Release 2008 January 23 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

A crafted IP packet vulnerability exists in the Cisco PIX 500 Series Security Appliance (PIX) and the Cisco 5500 Series Adaptive Security Appliance (ASA) that may result in a reload of the device. This vulnerability is triggered during processing of a crafted IP packet when the Time-to-Live (TTL) decrement feature is enabled.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0028 has been assigned to this vulnerability.

Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080123-asa.shtml>.

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

## ☐ Affected Products

### ☐ Vulnerable Products

The TTL decrement feature was introduced in version 7.2(2) and it is disabled by default. The Cisco PIX and ASA security appliances running software versions prior to 7.2(3)006 or 8.0(3) and that have the TTL decrement feature enabled are vulnerable.

By default the PIX and ASA security appliance software does not decrement the TTL of transient packets. The ability to decrement the TTL of transient packets can be enabled on a selective or global basis by using the **set connection decrement-ttl** command in the policy-map class configuration mode. To determine whether you are running this feature use the **show running-config** command and search for the **set connection decrement-ttl** command. Alternatively you can use the include argument to search for this command as follows:

```
ASA#show running-config | include decrement-ttl
set connection decrement-ttl
ASA#
```

The **set connection decrement-ttl** command is part of a configured class-map. In order for this command to take effect it must be applied using a policy-map (assigned globally or to an interface). For more information about the Modular Policy Framework on the Cisco ASA and PIX refer to the following link:

<http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/mpc.html>

To determine whether you are running a vulnerable version of Cisco PIX or ASA software, issue the **show version** command-line interface (CLI) command. The following example shows a Cisco ASA Security Appliance that runs software release 7.2(3):

```
ASA#show version

Cisco Adaptive Security Appliance Software Version 7.2(3)

[...]
```

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. The version notation is similar to the following:

```
PIX Version 7.2(3)
```

## ☐ Products Confirmed Not Vulnerable

Cisco PIX and ASA security appliances which do not support the TTL decrement feature or are not explicitly configured for it are not vulnerable.

**Note:** The TTL decrement feature was introduced in version 7.2(2), and it is disabled by default. The Cisco Firewall Services Module (FWSM) is not vulnerable.

No other Cisco products are currently known to be affected by this vulnerability.

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

## ☐ Details

A crafted IP packet vulnerability exists in the Cisco PIX 500 Series Security Appliance (PIX) and the Cisco 5500 Series Adaptive Security Appliance (ASA) that may result in a reload of the device. This vulnerability is triggered during processing of a crafted IP packet when the Time-to-Live (TTL) decrement feature is enabled. This vulnerability is documented in Cisco Bug ID [CSCsk48199](#) (**registered customers only**).

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

## ☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerability 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>.

<b>CSCsk48199 - Cisco PIX and ASA TTL Vulnerability</b>
<b>Calculate the environmental score of <a href="#">CSCsk48199</a></b>
CVSS Base Score - <b>7.8</b>

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

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

## Impact

Successful exploitation of the vulnerability described in this advisory will result in a reload of the affected device. Repeated exploitation can result in a sustained denial of service (DoS) condition.

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

## Software Versions and Fixes

This vulnerability is fixed in software version 7.2(3)6 or 8.0(3) and later.

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.

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

## Workarounds

Disable the TTL decrement feature using the **no set connection decrement-ttl** command in class configuration mode.

```
ASA(config)#policy-map localpolicy1
ASA(config-pmap)#class local_server
ASA(config-pmap-c)#no set connection decrement-ttl
ASA(config-pmap-c)#exit
```

For additional information on identifying and mitigating TTL based attacks, please refer to the Cisco Applied Intelligence White Paper "TTL Expiry Attack Identification and Mitigation", available at: <http://cisco.com/web/about/security/intelligence/ttl-expiry.html>.

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

## ☐ **Obtaining Fixed Software**

Cisco has released free software updates that address this vulnerability. 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/products/prod\\_warranties\\_item09186a008088e31f.html](http://www.cisco.com/en/US/products/prod_warranties_item09186a008088e31f.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.

[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 vulnerability described in this advisory.

[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-20080123-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](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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 1.2	2008-April- 25	Updated CVSS link for <a href="#">CSCsk48199</a> .
Revision 1.0	2008- January-23	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](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)



Send

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

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

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