

# [NEWS] Cisco PIX Firewall Authentication Denial of Service

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0024.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 10/07/01

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Subject: [NEWS] Cisco PIX Firewall Authentication Denial of Service

Message-Id: <20011007175210.8CD91138C4@mail.der-keiler.de>

Date: Sun, 7 Oct 2001 19:52:10 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

-----

Cisco PIX Firewall Authentication Denial of Service

---

## SUMMARY

The Cisco Secure PIX Firewall AAA authentication feature, introduced in version 4.0, is vulnerable to a Denial of Service (DoS) attack initiated by authenticating users on the system. This vulnerability affects specific configurations and has been resolved in released versions of the PIX Firewall.

This vulnerability has been assigned Cisco bug ID CSCdt92339.

This vulnerability has been discussed in our previous advisory:

<<http://www.securiteam.com/securitynews/5DP0B0K41M.html>> PIX Firewall DoS

Vulnerability (aaa authentication). This advisory contains the vendor response and workaround information.

## DETAILS

Affected Products:

All users of Cisco Secure PIX Firewalls with software versions 4.0 up to and including 4.4(8), 5.0(3), 5.1(3), 5.2(2), and 5.3(1) with

## Securiteam: [NEWS] Cisco PIX Firewall Authentication Denial of

configurations using AAA authentication are at risk.

Affected configurations will have configuration lines that begin:  
pixfirewall# aaa authentication ...

Configurations not including aaa authentication are not affected. PIX Firewall software versions 6.0(1) and later are not affected.

The IOS Firewall feature set is not affected by the above defect.

No other Cisco products are affected by this defect.

### Impact:

This issue causes a PIX Firewall to be vulnerable to a DoS attack in which the availability of the unit is degraded. This does not result in a loss in confidentiality or in loss of integrity of the traffic being filtered.

### Software versions and fixes:

A table of software versions and their fixes is available at:

~~<http://www.cisco.com/warp/public/707/pixfirewall-authen-flood-pub.shtml#Software>~~  
<http://www.cisco.com/warp/public/707/pixfirewall-authen-flood-pub.shtml#Software>

### Obtaining fixed software:

Cisco is offering free software upgrades to remedy this vulnerability for all affected customers. Customers with service contracts may upgrade to any software version. Customers without contracts may upgrade only within a single row of the table above, except that any available fixed software will be provided to any customer who can use it and for whom the standard fixed software is not yet available. As always, customers may install only the feature sets they have purchased.

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained via the Software Center on Cisco's Worldwide Web site at <http://www.cisco.com>. Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for assistance with the upgrade, which should be free of charge.

### Workarounds:

There is no known workaround for all authentication types.

If authentication is configured in conjunction with the Virtual HTTP feature, a limit of three concurrent authentication attempts per user exists, which could prevent this denial of service for HTTP traffic only. This would have no effect on authentication attempts for FTP or Telnet if the PIX is configured for authentication of those services.

### ADDITIONAL INFORMATION

Securiteam: [NEWS] Cisco PIX Firewall Authentication Denial of

The information has been provided by <mailto:[psirt@cisco.com](mailto:psirt@cisco.com)> Cisco  
Systems Product Security Incident Response Team.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NEWS] Oracle Application Server Discloses Full Path for Missing JSP Files"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)