



# CVE-2008-2057

Published on: 06/04/2008 12:00:00 AM UTC

Last Modified on: 08/11/2023 07:03:00 PM UTC

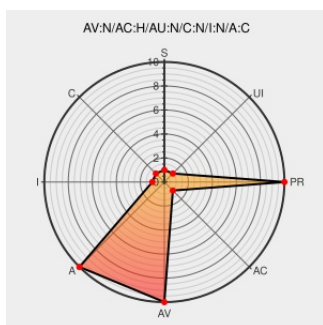
## CVE-2008-2057

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Adaptive Security Appliance Software](#) from [Cisco](#) contain the following vulnerability:

The Instant Messenger (IM) inspection engine in Cisco Adaptive Security Appliance (ASA) and Cisco PIX security appliance 7.2.x before 7.2(4), 8.0.x before 8.0(3)10, and 8.1.x before 8.1(1)2 allows remote attackers to cause a denial of service via a crafted packet.

CVE-2008-2057 has been assigned by [psirt@cisco.com](#) to track the vulnerability

CVSS2 Score: **5.4 - MEDIUM**

Access  
Vector

Access  
Complexity

Authentication

**NETWORK**

**HIGH**

**NONE**

Confidentiality  
Impact

Integrity  
Impact

Availability  
Impact

**NONE**

**NONE**

**COMPLETE**

## CVE References

Description

Tags

Link

Cisco PIX Firewall Bug in IM Inspection Engine Lets Remote Users Deny Service - SecurityTracker

[securitytracker.com](#)  
text/html

[SECTrack 1020180](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)  
text/html

[XF cisco-asa-pix-im-dos\(42837\)](#)

Cisco ASA and PIX Security Appliances Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

[web.archive.org](#)  
text/html

[SECUNIA 30552](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)  
text/html

[VUPEN ADV-2008-1750](#)

Cisco ASA Bug in IM Inspection Engine Lets Remote Users Deny Service - SecurityTracker

[securitytracker.com](#)  
text/html

[SECTrack 1020181](#)

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

[Patch](#)  
[www.cisco.com](#)

[CISCO 20080604 Multiple Vulnerabilities in Cisco PIX](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

#### Known Affected Configurations (CPE V2.3)

| Type                                                                                         | Vendor                | Product                                              | Version | Update | Edition | Language |
|----------------------------------------------------------------------------------------------|-----------------------|------------------------------------------------------|---------|--------|---------|----------|
| Application                                                                                  | <a href="#">Cisco</a> | <a href="#">Adaptive Security Appliance Software</a> | 7.2.2   | All    | All     | All      |
| Application                                                                                  | <a href="#">Cisco</a> | <a href="#">Adaptive Security Appliance Software</a> | 8.0     | All    | All     | All      |
| Operating System                                                                             | <a href="#">Cisco</a> | <a href="#">Adaptive Security Appliance Software</a> | 7.2.2   | All    | All     | All      |
| Operating System                                                                             | <a href="#">Cisco</a> | <a href="#">Adaptive Security Appliance Software</a> | 8.0     | All    | All     | All      |
| Application                                                                                  | <a href="#">Cisco</a> | <a href="#">Adaptive Security Appliance Software</a> | 7.2.2   | All    | All     | All      |
| Application                                                                                  | <a href="#">Cisco</a> | <a href="#">Adaptive Security Appliance Software</a> | 8.0     | All    | All     | All      |
| Hardware  | <a href="#">Cisco</a> | <a href="#">Pix Security Appliance</a>               | 7.2     | All    | All     | All      |
| Hardware  | <a href="#">Cisco</a> | <a href="#">Pix Security Appliance</a>               | 8.0     | All    | All     | All      |
| Hardware  | <a href="#">Cisco</a> | <a href="#">Pix Security Appliance</a>               | 7.2     | All    | All     | All      |
| Hardware  | <a href="#">Cisco</a> | <a href="#">Pix Security Appliance</a>               | 8.0     | All    | All     | All      |

cpe:2.3:a:cisco:adaptive\_security\_appliance\_software:7.2.2:\*\*\*\*\*:

cpe:2.3:a:cisco:adaptive\_security\_appliance\_software:8.0:\*\*\*\*\*:

cpe:2.3:o:cisco:adaptive\_security\_appliance\_software:7.2.2:\*\*\*\*\*:

cpe:2.3:o:cisco:adaptive\_security\_appliance\_software:8.0:\*\*\*\*\*:

cpe:2.3:a:cisco:adaptive\_security\_appliance\_software:7.2.2:\*\*\*\*\*:

cpe:2.3:a:cisco:adaptive\_security\_appliance\_software:8.0:\*\*\*\*\*:

cpe:2.3:h:cisco:pix\_security\_appliance:7.2:\*\*\*\*\*:

cpe:2.3:h:cisco:pix\_security\_appliance:8.0:\*\*\*\*\*:

cpe:2.3:h:cisco:pix\_security\_appliance:7.2:\*\*\*\*\*:

cpe:2.3:h:cisco:pix\_security\_appliance:8.0:\*\*\*\*\*:

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)