



CVE-2007-5569

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2007-5569
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-10-18 21:17:00 UTC
Updated	2023-08-11 19:02:00 UTC
Description	Cisco PIX and ASA appliances with 7.1 and 7.2 software, when configured for TLS sessions to the device, allow remote att

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Adaptive Security Appliance	7.2	All	All	All
Hardware	Cisco	Adaptive Security Appliance	7.2	All	All	All
Application	Cisco	Adaptive Security Appliance Software	7.1	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	7.1	All	All	All
Application	Cisco	Adaptive Security Appliance Software	7.1	All	All	All
Hardware	Cisco	Pix 500	All	7.1_software	All	All
Hardware	Cisco	Pix 500	All	7.2_software	All	All
Hardware	Cisco	Pix 500	All	7.1_software	All	All
Hardware	Cisco	Pix 500	All	7.2_software	All	All

References

Reference	Source	Link
Cisco Security Advisory: Multiple Vulnerabilities in Cisco PIX and ASA Appliance - Cisco Systems	CISCO	www.cisco.com
Cisco PIX and ASA TLS/MGCP Packet Processing Denial of Service - Advisories - Secunia	SECUNIA	secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Cisco ASA TLS and MGCP Processing Bugs Let Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytracker
Cisco PIX And ASA Appliances MGCP And TLS Packets Denial Of Service Vulnerabilities	BID	www.securityfocus.c

Cisco PIX Firewall TLS and MGCP Processing Bugs Let Remote Users Deny Service - SecurityTracker	SECTrack	www.securitytracker.com
IBM X-Force Exchange	XF	exchange.xforce.ibmsecurity.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://cve.report) 2026 |

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](http://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://mitre.org/cve). This site includes MITRE data granted under the following [license](http://mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report