



CVE-2007-2462

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

Summary

CVE	CVE-2007-2462
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-02 22:19:00 UTC
Updated	2023-08-11 19:02:00 UTC
Description	Unspecified vulnerability in Cisco Adaptive Security Appliance (ASA) and PIX 7.2 before 7.2(2)8, when using Layer 2 Tunneling Protocol (L2TP) over IPsec, could allow an attacker to bypass authentication and gain access to the device. The vulnerability is due to a buffer overflow in the L2TP authentication process. An attacker could exploit this vulnerability by sending a specially crafted L2TP packet to the device, which would cause the device to crash or reboot. This could allow the attacker to gain access to the device and its configuration. Cisco has released a software update to address this vulnerability. Users are advised to upgrade to the latest version of the software as soon as possible.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
35331	OSVDB	www.osvdb.org
Cisco PIX Bugs Let Remote Users Bypass LDAP Authentication and Deny Service - SecurityTracker	SECTrack	www.securitytracker.com
Cisco Security Advisory: LDAP and VPN Vulnerabilities in PIX and ASA Appliances - Cisco Systems	CISCO	www.cisco.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Cisco PIX and ASA Denial of Service and Security Bypass - Advisories - Secunia	SECUNIA	secunia.com

US-CERT Vulnerability Note VU#210876	CERT-VN	www.kb.cert.org
Cisco PIX And ASA Appliances Multiple Remote Vulnerabilities	BID	www.securityfocus.com
Cisco ASA Bugs Let Remote Users Bypass LDAP Authentication and Deny Service - SecurityTracker	SECTrack	www.securitytracker.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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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