



CVE-2007-2461

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

Summary

CVE	CVE-2007-2461
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	The DHCP relay agent in Cisco Adaptive Security Appliance (ASA) and PIX 7.2 allows remote attackers to cause a denial of service (DoS) by sending a large number of DHCP requests to the relay agent, which then forwards them to the upstream DHCP server. This can cause the upstream server to become overloaded and stop responding to legitimate requests.

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	7.2.2	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	7.2.2	All	All	All
Application	Cisco	Adaptive Security Appliance Software	7.2.2	All	All	All
Hardware	Cisco	Pix	7.2	All	All	All
Hardware	Cisco	Pix	7.2	All	All	All

References

Reference	Source
Cisco ASA DHCP Relay Agent Lets Remote Users Deny Service - SecurityTracker	SECT
Cisco PIX/ASA DHCP Relay Remote Denial of Service Vulnerability	BID
Cisco PIX Firewall DHCP Relay Agent Lets Remote Users Deny Service - SecurityTracker	SECT
Cisco Security Response: DHCP Relay Agent Vulnerability in Cisco PIX and ASA Appliances [Products & Services] - Cisco Systems	CISCO
35330	OSVD
IBM X-Force Exchange	XF
Cisco PIX and ASA Denial of Service and Security Bypass - Advisories - Secunia	SECU
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPE
US-CERT Vulnerability Note VU#530057	CERT

CVE Program record	CVE.C
NVD vulnerability detail	NVD
No vendor comments have been submitted for this CVE.	
There are currently no legacy QID mappings associated with this CVE.	

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). 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](#)