



CVE-2007-0244

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2007-0244
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-11 04:19:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	pptpgre.c in PoPToP Point to Point Tunneling Server (pptpd) before 1.3.4 allows remote attackers to cause a denial of serv

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	4.0	All	All	All

Operating System	Debian	Debian Linux	4.0	All	alpha	All
Operating System	Debian	Debian Linux	4.0	All	amd64	All
Operating System	Debian	Debian Linux	4.0	All	arm	All
Operating System	Debian	Debian Linux	4.0	All	hppa	All
Operating System	Debian	Debian Linux	4.0	All	ia-32	All
Operating System	Debian	Debian Linux	4.0	All	ia-64	All
Operating System	Debian	Debian Linux	4.0	All	m68k	All
Operating System	Debian	Debian Linux	4.0	All	mips	All
Operating System	Debian	Debian Linux	4.0	All	mipsel	All
Operating System	Debian	Debian Linux	4.0	All	powerpc	All
Operating System	Debian	Debian Linux	4.0	All	s390	All
Operating System	Debian	Debian Linux	4.0	All	sparc	All
Application	Poptop	Pptp Server	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference			Source		Link	
Security Announcement			af854a3a-2127-422b-91ae-364da2661108		www	
Debian -- Security Information -- DSA-1288-1 pptpd			af854a3a-2127-422b-91ae-364da2661108		www	
PPTPD: Denial of Service attack — Gentoo Linux Documentation			af854a3a-2127-422b-91ae-364da2661108		secu	
USN-459-1: pptpd vulnerability Ubuntu			af854a3a-2127-422b-91ae-364da2661108		ww	
SUSE Updates for Multiple Packages - Advisories - Secunia			af854a3a-2127-422b-91ae-364da2661108		secu	
Security Announcement			af854a3a-2127-422b-91ae-364da2661108		ww	
SourceForge.net: Poptop: Files			af854a3a-2127-422b-91ae-364da2661108		sou	
www.trustix.org/errata/2007/0017			af854a3a-2127-422b-91ae-364da2661108		ww	
PoPToP Sequence and Dequeing Bugs Let Remote Users Deny Service - SecurityTracker			af854a3a-2127-422b-91ae-364da2661108		ww	
PopTop PPTP Server GRE Packet Denial Of Service Vulnerability			af854a3a-2127-422b-91ae-364da2661108		ww	
Webmail - OVH			af854a3a-2127-422b-91ae-364da2661108		ww	
SUSE Update for Multiple Packages - Advisories - Secunia			af854a3a-2127-422b-91ae-364da2661108		secu	
USN-459-2: pptpd regression Ubuntu			af854a3a-2127-422b-91ae-364da2661108		ww	
Trustix Updates for Multiple Packages - Advisories - Secunia			af854a3a-2127-422b-91ae-364da2661108		secu	
CVE Program record			CVE.ORG		ww	
NVD vulnerability detail			NVD		nvc	

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](#)