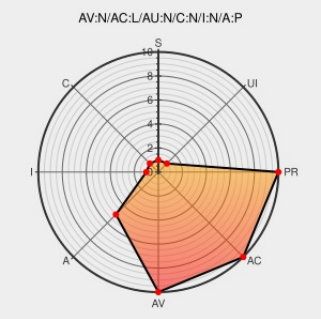
CVE-2005-1127

Published on: 04/16/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1127

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Postgrey from Postgrey contain the following vulnerability:

Format string vulnerability in the log function in Net::Server 0.87 and earlier, as used in Postfix Greylisting Policy Server (Postgrey) 1.18 and earlier, and possibly other products, allows remote attackers to cause a denial of service (crash) via format string specifiers that are not properly handled before being sent to syslog, as demonstrated using sender addresses to Postgrey.

CVE-2005-1127 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-1121-1 postgrey	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-1121
Gentoo Linux Documentation -- Net::Server: Format string vulnerability	www.gentoo.org, text/html	GENTOO GLSA-200608-18
No Description Provided	marc.info, text/html	FULLDISC 20050415 Use of function "log" in Perl module Net::Server
Rob Brown Net-Server Perl Module Logging Function Format String Vulnerability	cve.report (archive), text/html	BID 13193

[postgrey] Problem with crashing postgrey	web.archive.org text/html Inactive Link Not Archived	MLIST [postgrey] 20050414 Problem with crashing postgrey
[postgrey] ANNOUNCE: Postgrey 1.21 (SECURITY)	Patch web.archive.org text/html Inactive Link Not Archived	MLIST [postgrey] 20050414 ANNOUNCE: Postgrey 1.21 (SECURITY)
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 15517
Net::Server Log Format String Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 21149
Advisories - Mandriva Linux	www.mandriva.com text/html	MANDRIVA MDKSA-2006:131
[postgrey] Re: Problem with crashing postgrey	web.archive.org text/html Inactive Link Not Archived	MLIST [postgrey] 20050414 Re: Problem with crashing postgrey
Debian -- Security Information -- DSA-1122-1 libnet-server-perl	www.debian.org Depreciated Link text/html	DEBIAN DSA-1122
Debian update for libnet-server-perl - Advisories - Secunia	web.archive.org text/html	SECUNIA 21152
Secunia - Advisories - Gentoo update for net-server	web.archive.org text/html	SECUNIA 21452
Secunia - Advisories - Postgrey Format String Denial of Service Vulnerability	Patch web.archive.org text/html	SECUNIA 14958
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF postgrey-logging-dos(20108)
Debian update for postgrey - Advisories - Secunia	web.archive.org text/html	SECUNIA 21164

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postgrey	Postgrey	1.17	All	All	All
Application	Postgrey	Postgrey	1.18	All	All	All
Application	Postgrey	Postgrey	1.17	All	All	All
Application	Postgrey	Postgrey	1.18	All	All	All
Application	Postgrey	Postgrey	All	All	All	All

cpe:2.3:a:postgrey:postgrey:1.17:*:*:*:*:*:*:*:

cpe:2.3:a:postgrey:postgrey:1.18:*:*:*:*:*:*:*:

cpe:2.3:a:postgrey:postgrey:1.17:*:*:*:*:*:*:*:

cpe:2.3:a:postgrey:postgrey:1.18:*:*:*:*:*:*:*:

cpe:2.3:a:postgrey:postgrey:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© 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 registred 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