



CVE-2009-3229

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

Summary

CVE	CVE-2009-3229
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-09-17 10:30:00 UTC
Updated	2018-10-10 19:43:00 UTC
Description	The core server component in PostgreSQL 8.4 before 8.4.1, 8.3 before 8.3.8, and 8.2 before 8.2.14 allows remote authentication

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postgresql	Postgresql	8.2	All	All	All
Application	Postgresql	Postgresql	8.2.1	All	All	All
Application	Postgresql	Postgresql	8.2.10	All	All	All
Application	Postgresql	Postgresql	8.2.11	All	All	All
Application	Postgresql	Postgresql	8.2.12	All	All	All
Application	Postgresql	Postgresql	8.2.13	All	All	All
Application	Postgresql	Postgresql	8.2.2	All	All	All
Application	Postgresql	Postgresql	8.2.3	All	All	All
Application	Postgresql	Postgresql	8.2.4	All	All	All
Application	Postgresql	Postgresql	8.2.5	All	All	All
Application	Postgresql	Postgresql	8.2.6	All	All	All
Application	Postgresql	Postgresql	8.2.7	All	All	All
Application	Postgresql	Postgresql	8.2.8	All	All	All
Application	Postgresql	Postgresql	8.2.9	All	All	All
Application	Postgresql	Postgresql	8.3	All	All	All
Application	Postgresql	Postgresql	8.3.1	All	All	All
Application	Postgresql	Postgresql	8.3.2	All	All	All

[SECURITY] Fedora 11 Update: postgresql-8.3.8-1.fc11	FEDORA	www.fedoraproject.org
PostgreSQL: Documentation: Manuals: PostgreSQL 8.3: Release 8.3.8	CONFIRM	www.postgresql.org
Fedora update for postgresql - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
[SECURITY] Fedora 10 Update: postgresql-8.3.8-1.fc10	FEDORA	www.fedoraproject.org
USN-834-1: PostgreSQL vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
Bug 522092 – CVE-2009-3229 postgresql: authenticated user server DoS via plugin re-LOAD-ing	CONFIRM	bugzilla.mandrillinux.com
Security Advisory SA36800 - Ubuntu update for postgresql - Secunia	SECUNIA	secunia.com
Debian update for postgresql - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
wiki.rpath.com/wiki/Advisories:rPSA-2010-0012	CONFIRM	wiki.rpath.com
PostgreSQL Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
PostgreSQL: Security Information	CONFIRM	www.postgresql.org
SecurityFocus	BUGTRAQ	www.securityfocus.com
270408	SUNALERT	sunsolve.sun.com
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:017	SUSE	lists.suse.com
Debian -- Security Information -- DSA-1900-1 postgresql-7.4, postgresql-8.1, postgresql-8.3, postgresql-8.4	DEBIAN	www.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-09-24	Tomas Hoger	Not vulnerable. This issue did not affect the versions of PostgreSQL as shipped with Red Hat Enterprise Linux 5.4 and 5.5.

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](#)