



CVE-2015-5289

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

Summary

CVE	CVE-2015-5289
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-26 14:59:00 UTC
Updated	2023-11-07 02:26:00 UTC
Description	Multiple stack-based buffer overflows in json parsing in PostgreSQL before 9.3.x before 9.3.10 and 9.4.x before 9.4.5 allow

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Postgresql	Postgresql	All	All	All	All
Application	Postgresql	Postgresql	9.1	All	All	All
Application	Postgresql	Postgresql	9.1.1	All	All	All
Application	Postgresql	Postgresql	9.1.10	All	All	All
Application	Postgresql	Postgresql	9.1.11	All	All	All
Application	Postgresql	Postgresql	9.1.12	All	All	All
Application	Postgresql	Postgresql	9.1.13	All	All	All
Application	Postgresql	Postgresql	9.1.14	All	All	All
Application	Postgresql	Postgresql	9.1.15	All	All	All
Application	Postgresql	Postgresql	9.1.16	All	All	All
Application	Postgresql	Postgresql	9.1.17	All	All	All
Application	Postgresql	Postgresql	9.1.18	All	All	All

Table 1: Application Data						
Application	Postgresql	Postgresql	9.1.2	All	All	All
Application	Postgresql	Postgresql	9.1.3	All	All	All
Application	Postgresql	Postgresql	9.1.4	All	All	All
Application	Postgresql	Postgresql	9.1.5	All	All	All
Application	Postgresql	Postgresql	9.1.6	All	All	All
Application	Postgresql	Postgresql	9.1.7	All	All	All
Application	Postgresql	Postgresql	9.1.8	All	All	All
Application	Postgresql	Postgresql	9.1.9	All	All	All
Application	Postgresql	Postgresql	9.2	All	All	All
Application	Postgresql	Postgresql	9.2.1	All	All	All
Application	Postgresql	Postgresql	9.2.10	All	All	All
Application	Postgresql	Postgresql	9.2.11	All	All	All
Application	Postgresql	Postgresql	9.2.12	All	All	All
Application	Postgresql	Postgresql	9.2.13	All	All	All
Application	Postgresql	Postgresql	9.2.2	All	All	All
Application	Postgresql	Postgresql	9.2.3	All	All	All
Application	Postgresql	Postgresql	9.2.4	All	All	All
Application	Postgresql	Postgresql	9.2.5	All	All	All
Application	Postgresql	Postgresql	9.2.6	All	All	All
Application	Postgresql	Postgresql	9.2.7	All	All	All
Application	Postgresql	Postgresql	9.2.8	All	All	All
Application	Postgresql	Postgresql	9.2.9	All	All	All
Application	Postgresql	Postgresql	9.3	All	All	All
Application	Postgresql	Postgresql	9.3.1	All	All	All
Application	Postgresql	Postgresql	9.3.2	All	All	All
Application	Postgresql	Postgresql	9.3.3	All	All	All
Application	Postgresql	Postgresql	9.3.4	All	All	All
Application	Postgresql	Postgresql	9.3.5	All	All	All
Application	Postgresql	Postgresql	9.3.6	All	All	All
Application	Postgresql	Postgresql	9.3.7	All	All	All
Application	Postgresql	Postgresql	9.3.8	All	All	All
Application	Postgresql	Postgresql	9.3.9	All	All	All
Application	Postgresql	Postgresql	9.4.0	All	All	All
Application	Postgresql	Postgresql	9.4.1	All	All	All
Application	Postgresql	Postgresql	9.4.2	All	All	All

Application	Postgresql	Postgresql	9.3	All	All	All
Application	Postgresql	Postgresql	9.3.1	All	All	All
Application	Postgresql	Postgresql	9.3.2	All	All	All
Application	Postgresql	Postgresql	9.3.3	All	All	All
Application	Postgresql	Postgresql	9.3.4	All	All	All
Application	Postgresql	Postgresql	9.3.5	All	All	All
Application	Postgresql	Postgresql	9.3.6	All	All	All
Application	Postgresql	Postgresql	9.3.7	All	All	All
Application	Postgresql	Postgresql	9.3.8	All	All	All
Application	Postgresql	Postgresql	9.3.9	All	All	All
Application	Postgresql	Postgresql	9.4.0	All	All	All
Application	Postgresql	Postgresql	9.4.1	All	All	All
Application	Postgresql	Postgresql	9.4.2	All	All	All
Application	Postgresql	Postgresql	9.4.3	All	All	All
Application	Postgresql	Postgresql	9.4.4	All	All	All
Application	Postgresql	Postgresql	All	All	All	All

References						
Reference			Source			
git.postgresql.org Git - postgresql.git/commit			CONFIRM			
PostgreSQL: Documentation: 9.3: Release 9.3.10			CONFIRM			
[SECURITY] Fedora 22 Update: postgresql-9.4.5-1.fc22			FEDORA			
PostgreSQL: Multiple vulnerabilities (GLSA 201701-33) — Gentoo security			GENTOO			
USN-2772-1: PostgreSQL vulnerabilities Ubuntu			UBUNTU			
PostgreSQL: 2015-10-08 Security Update Release			CONFIRM			
[SECURITY] Fedora 23 Update: postgresql-9.4.5-1.fc23			FEDORA			
PostgreSQL: Documentation: 9.4: Release 9.4.5			CONFIRM			
[security-announce] SUSE-SU-2016:0677-1: important: Security update for			SUSE			
PostgreSQL CVE-2015-5289 Remote Denial Of Service Vulnerability			BID			
Oracle Linux Bulletin - October 2015			CONFIRM			
PostgreSQL Bugs Let Remote Users Deny Service and May Let Remote Users Obtain Portions of Memory - SecurityTracker			SECTrack			
openSUSE-SU-2015:1907-1: moderate: Security update for postgresql93			SUSE			
Debian -- Security Information -- DSA-3374-1 postgresql-9.4			DEBIAN			
git.postgresql.org Git - postgresql.git/commit						
CVE Program record			CVE.ORG			
NVD vulnerability detail			NVD			

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710501 Gentoo Linux PostgreSQL Multiple Vulnerabilities (GLSA 201701-33)

© [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](#)