



CVE-2014-0066

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

Summary

CVE	CVE-2014-0066
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-31 14:58:00 UTC
Updated	2023-02-13 00:31:00 UTC
Description	The chkpass extension in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.4 is vulnerable to a buffer overflow attack.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postgresql	Postgresql	8.4.1	All	All	All
Application	Postgresql	Postgresql	8.4.10	All	All	All
Application	Postgresql	Postgresql	8.4.11	All	All	All
Application	Postgresql	Postgresql	8.4.12	All	All	All
Application	Postgresql	Postgresql	8.4.13	All	All	All
Application	Postgresql	Postgresql	8.4.14	All	All	All
Application	Postgresql	Postgresql	8.4.15	All	All	All
Application	Postgresql	Postgresql	8.4.16	All	All	All
Application	Postgresql	Postgresql	8.4.17	All	All	All
Application	Postgresql	Postgresql	8.4.18	All	All	All
Application	Postgresql	Postgresql	8.4.2	All	All	All
Application	Postgresql	Postgresql	8.4.3	All	All	All
Application	Postgresql	Postgresql	8.4.4	All	All	All
Application	Postgresql	Postgresql	8.4.5	All	All	All
Application	Postgresql	Postgresql	8.4.6	All	All	All
Application	Postgresql	Postgresql	8.4.7	All	All	All
Application	Postgresql	Postgresql	8.4.8	All	All	All

Application	Postgresql	Postgresql	8.4.9	All	All	All
Application	Postgresql	Postgresql	9.0	All	All	All
Application	Postgresql	Postgresql	9.0.1	All	All	All
Application	Postgresql	Postgresql	9.0.10	All	All	All
Application	Postgresql	Postgresql	9.0.11	All	All	All
Application	Postgresql	Postgresql	9.0.12	All	All	All
Application	Postgresql	Postgresql	9.0.13	All	All	All
Application	Postgresql	Postgresql	9.0.14	All	All	All
Application	Postgresql	Postgresql	9.0.15	All	All	All
Application	Postgresql	Postgresql	9.0.2	All	All	All
Application	Postgresql	Postgresql	9.0.3	All	All	All
Application	Postgresql	Postgresql	9.0.4	All	All	All
Application	Postgresql	Postgresql	9.0.5	All	All	All
Application	Postgresql	Postgresql	9.0.6	All	All	All
Application	Postgresql	Postgresql	9.0.7	All	All	All
Application	Postgresql	Postgresql	9.0.8	All	All	All
Application	Postgresql	Postgresql	9.0.9	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	9.1.2	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	9.2.2	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	9.0.7	All	All	All
Application	Postgresql	Postgresql	9.0.8	All	All	All
Application	Postgresql	Postgresql	9.0.9	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	9.1.2	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	9.2.2	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	9.3	All	All	All
Application	Postgresql	Postgresql	9.3.1	All	All	All
Application	Postgresql	Postgresql	9.3.2	All	All	All
Application	Postgresql	Postgresql	All	All	All	All

References						
Reference				Source	Link	Tags
USN-2120-1: PostgreSQL vulnerabilities Ubuntu				UBUNTU	www.ubuntu.com	
Red Hat Customer Portal				MISC	access.redhat.com	
Debian -- Security Information -- DSA-2865-1 postgresql-9.1				DEBIAN	www.debian.org	
Red Hat Customer Portal				REDHAT	rhn.redhat.com	
Red Hat Customer Portal				REDHAT	rhn.redhat.com	
Red Hat Customer Portal				REDHAT	rhn.redhat.com	
NEOHAPSIS - Peace of Mind Through Integrity and Insight				APPLE	archives.neohapsis.com	

Red Hat Customer Portal	MISC	access.redhat.com	
Red Hat Customer Portal	MISC	access.redhat.com	
PostgreSQL: PostgreSQL 9.3.3, 9.2.7, 9.1.12, 9.0.16 and 8.4.20 released!	CONFIRM	www.postgresql.org	Vendor
Bug 1065236 – CVE-2014-0066 postgresql: NULL pointer dereference	MISC	bugzilla.redhat.com	
openSUSE-SU-2014:0368-1: moderate: postgresql: updates to 9.0.16 securit	SUSE	lists.opensuse.org	
access.redhat.com CVE-2014-0066	MISC	access.redhat.com	
About the security content of OS X Server v3.2.1 - Apple Support	CONFIRM	support.apple.com	
Red Hat Customer Portal	MISC	access.redhat.com	
About the security content of OS X Server v4.0 - Apple Support	CONFIRM	support.apple.com	
Debian -- Security Information -- DSA-2864-1 postgresql-8.4	DEBIAN	www.debian.org	
20140220securityrelease - PostgreSQL wiki	CONFIRM	wiki.postgresql.org	Vendor
Red Hat Customer Portal	REDHAT	rhn.redhat.com	
Oracle Critical Patch Update - October 2017	CONFIRM	www.oracle.com	
Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView	CONFIRM	kb.juniper.net	
openSUSE-SU-2014:0345-1: moderate: postgresql92: update to 9.2.7 securit	SUSE	lists.opensuse.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report