



# CVE-2018-10915

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

## Summary

<b>CVE</b>	CVE-2018-10915
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-08-09 20:29:00 UTC
<b>Updated</b>	2021-08-04 17:14:00 UTC
<b>Description</b>	A vulnerability was found in libpq, the default PostgreSQL client library where libpq failed to properly reset its internal state I

## Risk And Classification

### Problem Types: CWE-89

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Postgresql</a>	<a href="#">Postgresql</a>	All	All	All	All
Application	<a href="#">Postgresql</a>	<a href="#">Postgresql</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.5	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	12	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	12.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	13	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	13.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	12.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	13.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Virtualization</a>	4.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Virtualization</a>	4.0	All	All	All

## References

### Reference

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[1609891 – \(CVE-2018-10915\) CVE-2018-10915 postgresql: Certain host connection parameters defeat client-side security defenses](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[PostgreSQL CVE-2018-10915 Security Bypass Vulnerability](#)

[\[SECURITY\] \[DLA 1464-1\] postgresql-9.4 security update](#)

[PostgreSQL: Multiple vulnerabilities \(GLSA 201810-08\) — Gentoo security](#)

[USN-3744-1: PostgreSQL vulnerabilities | Ubuntu security notices | Ubuntu](#)

[Red Hat Customer Portal](#)

[PostgreSQL: PostgreSQL 10.5, 9.6.10, 9.5.14, 9.4.19, 9.3.24, and 11 Beta 3 Released!](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[\[security-announce\] openSUSE-SU-2020:1227-1: moderate: Security update f](#)

[PostgreSQL Bugs Let Remote Authenticated Users Access Systems and Obtain Potentially Sensitive Information from System Memory - Secu](#)

[Debian -- Security Information -- DSA-4269-1 postgresql-9.6](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

500533 Alpine Linux Security Update for postgresql

502001 Alpine Linux Security Update for postgresql14

502767 Alpine Linux Security Update for postgresql15

504300 Alpine Linux Security Update for postgresql14

710227 Gentoo Linux PostgreSQL Multiple Vulnerabilities (GLSA 201810-08)

© [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](#)