



# CVE-2020-25694

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

## Summary

<b>CVE</b>	CVE-2020-25694
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-11-16 01:15:00 UTC
<b>Updated</b>	2022-10-19 15:00:00 UTC
<b>Description</b>	A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.12. An attacker can connect to the database and downgrade the connection security settings to none, which allows the attacker to bypass the database's security settings and access sensitive data.

## Risk And Classification

**Problem Types:** CWE-327

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Postgresql	Postgresql	All	All	All	All
Application	Postgresql	Postgresql	All	All	All	All

## References

Reference	Source	Link
November 2020 PostgreSQL Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>
PostgreSQL: Multiple vulnerabilities (GLSA 202012-07) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
1894423 – (CVE-2020-25694) CVE-2020-25694 postgresql: Reconnection can downgrade connection security settings	MISC	<a href="#">bugzilla.redhat.com</a>
[SECURITY] [DLA 2478-1] postgresql-9.6 security update	MLIST	<a href="#">lists.debian.org</a>
PostgreSQL: Security Information	MISC	<a href="#">www.postgresql.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">159172</a> Oracle Enterprise Linux Security Update for postgresql (ELSA-2021-1512)
<a href="#">159270</a> Oracle Enterprise Linux Security Update for rh-postgresql10-postgresql (ELSA-2021-9290)
<a href="#">239266</a> Red Hat Update for postgresql (RHSA-2021:1512)
<a href="#">257093</a> CentOS Security Update for postgresql (CESA-2021:1512)
<a href="#">257095</a> CentOS Security Update for postgresql (CESA-2021:1512)
<a href="#">352389</a> Amazon Linux Security Advisory for postgresql: ALAS2-2021-1665
<a href="#">352472</a> Amazon Linux Security Advisory for postgresql92: ALAS-2021-1519
<a href="#">376872</a> Alibaba Cloud Linux Security Update for libpq (ALINUX3-SA-2021:0002)
<a href="#">377029</a> Alibaba Cloud Linux Security Update for postgresql (ALINUX2-SA-2021:0028)
<a href="#">377113</a> Alibaba Cloud Linux Security Update for postgresql:12 (ALINUX3-SA-2021:0017)
<a href="#">500540</a> Alpine Linux Security Update for postgresql
<a href="#">502008</a> Alpine Linux Security Update for postgresql14
<a href="#">502162</a> Alpine Linux Security Update for postgresql12
<a href="#">502774</a> Alpine Linux Security Update for postgresql15
<a href="#">504307</a> Alpine Linux Security Update for postgresql14
<a href="#">505666</a> Alpine Linux Security Update for postgresql15
<a href="#">671231</a> EulerOS Security Update for postgresql (EulerOS-SA-2022-1182)
<a href="#">671354</a> EulerOS Security Update for postgresql (EulerOS-SA-2022-1281)
<a href="#">730155</a> McAfee Web Gateway Multiple Vulnerabilities(WP-3580, WP-3656, WP-3815, WP-3878, WP-3882, WP-3934,WP-3935, WP-3936, WP-3999)
<a href="#">750347</a> OpenSUSE Security Update for postgresql, postgresql13 (openSUSE-SU-2021:0337-1)
<a href="#">750566</a> OpenSUSE Security Update for postgresql10 (openSUSE-SU-2020:2028-1)
<a href="#">750567</a> OpenSUSE Security Update for postgresql12 (openSUSE-SU-2020:2029-1)
<a href="#">750573</a> OpenSUSE Security Update for postgresql12 (openSUSE-SU-2020:2018-1)
<a href="#">750575</a> OpenSUSE Security Update for postgresql10 (openSUSE-SU-2020:2019-1)
<a href="#">900047</a> CBL-Mariner Linux Security Update for postgresql 12.1
<a href="#">902973</a> Common Base Linux Mariner (CBL-Mariner) Security Update for postgresql (3607)
<a href="#">940127</a> AlmaLinux Security Update for postgresql:10 (ALSA-2020:5567)
<a href="#">940130</a> AlmaLinux Security Update for postgresql:12 (ALSA-2020:5620)

[940246](#) AlmaLinux Security Update for libpq (ALSA-2020:5401)

[940299](#) AlmaLinux Security Update for postgresql:9.6 (ALSA-2020:5619)

[960242](#) Rocky Linux Security Update for postgresql:12 (RLSA-2020:5620)

© [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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)