CVE-2020-25695

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-25695
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-16 01:15:00 UTC
Updated	2022-10-19 15:01:00 UTC
Description	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.

Risk And Classification

Problem Types: CWE-89

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	L
November 2020 PostgreSQL Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	s
PostgreSQL: Multiple vulnerabilities (GLSA 202012-07) — Gentoo security	GENTOO	s
[SECURITY] [DLA 2478-1] postgresql-9.6 security update	MLIST	li
1894425 – (CVE-2020-25695) CVE-2020-25695 postgresql: Multiple features escape "security restricted operation" sandbox	MISC	b
PostgreSQL: Security Information	MISC	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159172 Oracle Enterprise Linux Security Update for postgresql (ELSA-2021-1512)

159270 Oracle Enterprise Linux Security Update for rh-postgresql10-postgresql (ELSA-2021-9290)

239266 Red Hat Update for postgresql (RHSA-2021:1512)

257093 CentOS Security Update for postgresql (CESA-2021:1512)

257095 CentOS Security Update for postgresql (CESA-2021:1512)

352389 Amazon Linux Security Advisory for postgresql: ALAS2-2021-1665

352472 Amazon Linux Security Advisory for postgresql92: ALAS-2021-1519

352821 Amazon Linux Security Advisory for postgresql9: AL2012-2021-345

377029 Alibaba Cloud Linux Security Update for postgresql (ALINUX2-SA-2021:0028)

377113 Alibaba Cloud Linux Security Update for postgresql:12 (ALINUX3-SA-2021:0017)

500540 Alpine Linux Security Update for postgresql

502008 Alpine Linux Security Update for postgresql14

502162 Alpine Linux Security Update for postgresql12

502774 Alpine Linux Security Update for postgresql15

504307 Alpine Linux Security Update for postgresql14

505666 Alpine Linux Security Update for postgresql15

670201 EulerOS Security Update for postgresql (EulerOS-SA-2021-1700)

670243 EulerOS Security Update for postgresql (EulerOS-SA-2021-1833)

670852 EulerOS Security Update for postgresql (EulerOS-SA-2021-1700)

730155 McAfee Web Gateway Multiple Vulnerabilities(WP-3580, WP-3656, WP-3815, WP-3878, WP-3882, WP-3934,WP-3935, WP-3936, WP-3999)

750347 OpenSUSE Security Update for postgresql, postgresql13 (openSUSE-SU-2021:0337-1)

750566 OpenSUSE Security Update for postgresql10 (openSUSE-SU-2020:2028-1)

750567 OpenSUSE Security Update for postgresql12 (openSUSE-SU-2020:2029-1)

750573 OpenSUSE Security Update for postgresql12 (openSUSE-SU-2020:2018-1)

750575 OpenSUSE Security Update for postgresql10 (openSUSE-SU-2020:2019-1)

900047 CBL-Mariner Linux Security Update for postgresql 12.1

902986 Common Base Linux Mariner (CBL-Mariner) Security Update for postgresql (3608)

940127 AlmaLinux Security Update for postgresql:10 (ALSA-2020:5567)

940130 AlmaLinux Security Update for postgresql:12 (ALSA-2020:5620)

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

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