

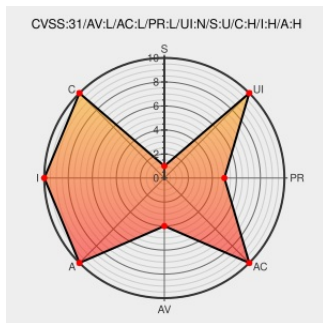


CVE-2019-10128

Published on: 03/19/2021 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:06:59 PM UTC

CVE-2019-10128

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Windows](#) from [Microsoft](#) contain the following vulnerability:

A vulnerability was found in postgresql versions 11.x prior to 11.3. The Windows installer for EnterpriseDB-supplied PostgreSQL does not lock down the ACL of the binary installation directory or the ACL of the data directory; it keeps the inherited ACL. In the default configuration, this allows a local attacker to read arbitrary data directory files, essentially bypassing database-imposed read access limitations. In plausible non-default configurations, an attacker having both an unprivileged Windows account and an unprivileged PostgreSQL account can cause the PostgreSQL service account to execute arbitrary code.

CVE-2019-10128 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4.1 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

1707102 – (CVE-2019-10128) CVE-2019-10128 postgresql: EnterpriseDB installer does not clear permissive ACL entries

[bugzilla.redhat.com](#)
text/html

MISC
[bugzilla.redhat.com/show_bug.cgi?id=1707102](#)

PostgreSQL: PostgreSQL 11.3, 10.8, 9.6.13, 9.5.17, and 9.4.22 Released!

[www.postgresql.org](#)
text/html

MISC
[www.postgresql.org/about/news/1939/](#)

March 2021 PostgreSQL Vulnerabilities in NetApp Products | NetApp Product Security

[security.netapp.com](#)
text/html

CONFIRM
[security.netapp.com/advisory/ntap-20210430-0004/](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Application	Postgresql	Postgresql	All	All	All	All
cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:						
cpe:2.3:a:postgresql:postgresql:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID →