

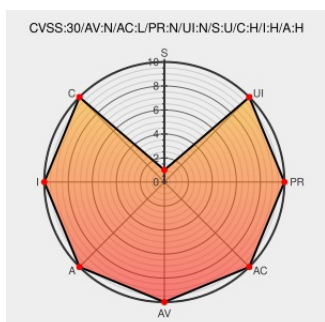


CVE-2018-16203

Published on: 01/09/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:34 PM UTC

CVE-2018-16203

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

Certain versions of [Pgpooladmin](#) from [Pgpool](#) contain the following vulnerability:

PgpoolAdmin 4.0 and earlier allows remote attackers to bypass the login authentication and obtain the administrative privilege of the PostgreSQL database via unspecified vectors.

CVE-2018-16203 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [PgPool Global Development Group](#) - [PgpoolAdmin](#) version **4.0 and earlier**

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
JVN#13199224: PgpoolAdmin fails to restrict access permissions	Third Party Advisory jvn.jp text/xml	JVN JVN#13199224

pgpool Wiki

Vendor Advisory

pgpool.net

text/html

MISC

pgpool.net/mediawiki/index.php/Main_Page

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
Application	Pgpool	Pgpooladmin	All	All	All	All

cpe:2.3:a:pgpool:pgpooladmin:*****::

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→