



CVE-2022-41946

Published on: Not Yet Published

Last Modified on: 11/28/2022 07:43:00 PM UTC

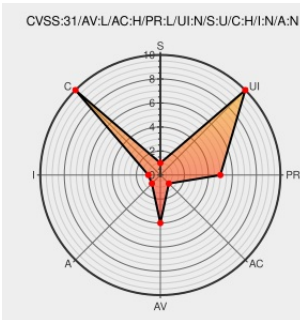
CVE-2022-41946 - advisory for GHSA-562r-vg33-8x8h

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Postgresql Jdbc Driver](#) from [Postgresql](#) contain the following vulnerability:

pgjdbc is an open source postgresql JDBC Driver. In affected versions a prepared statement using either `PreparedStatement.setText(int, InputStream)` or `PreparedStatement.setBytea(int, InputStream)` will create a temporary file if the `InputStream` is larger than 2k. This will create a temporary file which is readable by other users on Unix like

systems, but not MacOS. On Unix like systems, the system's temporary directory is shared between all users on that system. Because of this, when files and directories are written into this directory they are, by default, readable by other users on that same system. This vulnerability does not allow other users to overwrite the contents of these directories or files. This is purely an information disclosure vulnerability. Because certain JDK file system APIs were only added in JDK 1.7, this this fix is dependent upon the version of the JDK you are using. Java 1.7 and higher users: this vulnerability is fixed in 4.5.0. Java 1.6 and lower users: no patch is available. If you are unable to patch, or are stuck running on Java 1.6, specifying the `java.io.tmpdir` system environment variable to a directory that is exclusively owned by the executing user will mitigate this vulnerability.

CVE-2022-41946 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [pgjdbc](#) - [pgjdbc](#) version $\geq 42.2.0$, $< 42.2.27$

Affected Vendor/Software: [pgjdbc](#) - [pgjdbc](#) version $> 42.3.0$, $< 42.3.8$

Affected Vendor/Software: [pgjdbc](#) - [pgjdbc](#) version $\geq 42.4.0$, $< 42.4.3$

Affected Vendor/Software: [pgjdbc](#) - [pgjdbc](#) version $\geq 42.5.0$, $< 42.5.1$

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

LOCAL

LOW

LOW

NONE

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
Merge pull request from GHSA-562r-vg33-8x8h · pgjdbc/pgjdbc@9008dc9 · GitHub	github.com text/html	MISC github.com/pgjdbc/pgjdbc/commit/9008dc9aade6dbfe4efafcd6872ebc55f4699cf5
TemporaryFolder on unix-like systems does not limit access to created files · Advisory · pgjdbc/pgjdbc · GitHub	github.com text/html	CONFIRM github.com/pgjdbc/pgjdbc/security/advisories/GHSA-562r-vg33-8x8h

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	Postgresql	Postgresql Jdbc Driver	All	All	All	All
Application	Postgresql	Postgresql Jdbc Driver	42.5.0	-	All	All
Application	Postgresql	Postgresql Jdbc Driver	42.5.0	rc1	All	All
Application	Postgresql	Postgresql Jdbc Driver	All	All	All	All
Application	Postgresql	Postgresql Jdbc Driver	All	All	All	All

cpe:2.3:a:postgresql:postgresql_jdbc_driver:*:*:*:*:*:

cpe:2.3:a:postgresql:postgresql_jdbc_driver:42.5.0:-:*:*:*:*:

cpe:2.3:a:postgresql:postgresql_jdbc_driver:42.5.0:rc1:*:*:*:*:

cpe:2.3:a:postgresql:postgresql_jdbc_driver:*:*:*:*:*:

cpe:2.3:a:postgresql:postgresql_jdbc_driver:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@PostgreSQL	News: PostgreSQL JDBC 42.5.1, 42.4.3, 42.3.8, 42.2.27.jre7 Security update for CVE-2022-41946 postgresql.org/about/news/pos...	2022-11-23 17:30:03
@dev_talk	PostgreSQL JDBC 42.5.1, 42.4.3, 42.3.8, 42.2.27.jre7 Security update for CVE-2022-41946 forum.devtalk.com/t/84177... twitter.com/i/web/status/1...	2022-11-23 18:05:34

 @CVEreport	CVE-2022-41946 : pgjdbc is an open source postgresql JDBC Driver. In affected versions a prepared statement using e... twitter.com/i/web/status/1...	2022-11-23 20:04:25
 /r/netcve	CVE-2022-41946	2022-11-23 20:38:42

[← Previous ID](#)

[Next ID→](#)

© CVE.report 2022   |

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