National Cyber Security Centre

2403220153-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Vulnerability in the PostgreSQL JDBC Driver - pgJDBC CVSSv3.1: 10.0

Tuesday 26th March, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

PostgreSQL JDBC have released a fix to address a security issue: CVE-2024-1597.

pgJDBC, the PostgreSQL JDBC Driver, allows an attacker to inject SQL if using PreferQueryMode=SIMPLE. **Note this is not the default. In the default mode there is no vulnerability**. A placeholder for a numeric value must be immediately preceded by a minus. There must be a second placeholder for a string value after the first placeholder; both must be on the same line. By constructing a matching string payload, the attacker can inject SQL to alter the query, bypassing the protections that parameterized queries bring against SQL Injection attacks.

EPSS[1]**:** 0.129890000
(For up to date EPSS score click here: https://api.first.org/data/v1/epss?cve=CVE-2024-1597)

Products Affected

pgJDBC

- All versions prior to 42.7.2
- All versions prior to 42.6.1
- All versions prior to 42.5.5
- All versions prior to 42.3.9
- All versions prior to 42.2.28

EnterpriseDB pgJDBC

- All versions prior to 42.5.4.2

Impact

SQL injection is possible when using the non-default connection property **preferQueryMode=simple** in combination with application code that has vulnerable SQL that negates a parameter value. There is no vulnerability in the driver when using the default query mode. Users that do not override the query mode are not impacted.
Common Weakness Enumeration (CWE)[2]**:** Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from pgJDBC.

Additional recommendations and mitigation's for CVE-2024-1597 can be found in the respective link(s) below:
https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-24rp-q3w6-vc56
https://www.enterprisedb.com/docs/security/assessments/cve-2024-1597/
https://www.enterprisedb.com/docs/jdbc_connector/latest/01_jdbc_rel_notes/
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/TZQTSMESZD2RJ5XBPSXH3TIQVUW5DIUU/

[1] https://www.first.org/epss/articles/prob_percentile_bins
[2] https://cwe.mitre.org/

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie