Partial Path Traversal Vulnerability

Moderate **ncordon** published **GHSA-78f9-745f-278p** on Aug 11

Package

org.neo4j.procedure:apoc (Maven)

Affected versions

<4.4.0.8, <4.3.0.7, <4.2.0.12, <4.1.0.12, <3.5.0.20

Patched versions

4.4.0.8, 4.3.0.7

Description

Impact

A partial Directory Traversal Vulnerability found in `apoc.log.stream` function of apoc plugins in Neo4j Graph database.
This issue allows a malicious actor to potentially break out of the expected directory. The impact is limited to sibling directories. For example, `userControlled.getCanonicalPath().startsWith("/usr/out")` will allow an attacker to access a directory with a name like `/usr/outnot` .

Patches

The users should aim to use the latest released version compatible with their Neo4j version. The minimum versions containing patch for this vulnerability are 4.4.0.8 and 4.3.0.7

Workarounds

If you cannot upgrade the library, you can control the allowlist of the functions that can be used in your system

For more information

If you have any questions or comments about this advisory:

- Open an issue in neo4j-apoc-procedures
- Email us at security@neo4j.com

Credits

We want to publicly recognise the contribution of Jonathan Leitschuh for reporting this issue.

Severity

Moderate

CVE ID

CVE-2022-37423

Weaknesses

CWE-22

Credits

JLLeitschuh