SSRF and Data Modification via read_only Mode Bypass through CALL Procedures

Low **a-s-g93** published **GHSA-x3cv-r3g3-fpg9** 5 hours ago

Package

mcp-neo4j-cypher (pip)

Affected versions	Patched versions
<0.6.0	0.6.0

Description

Summary

The `read_only` mode in `mcp-neo4j-cypher` versions prior to 0.6.0 can be bypassed using `CALL` procedures.

Details

Impact

The enforcing of `read_only` mode in vulnerable versions could be bypassed by certain APOC procedures.

Patches

v0.6.0 release hardened the checks around the mode. The only way to guarantee the server actions is to limit the permissions of the db credentials available to the server.

Notes

Impacts for server-side request forgery vulnerabilities may depend on both the configuration of the vulnerable system as well as the presence of other systems in the environment that could be accessed as part of exploitation.

Recommended hardening

- Limit the apoc procedures to what's required
- Manage data loading privileges
- Don't relax the default settings without compensating controls
  - `apoc.import.file.enabled` is `false` by default
  - `apoc.import.file.use_neo4j_config` is `true` by default to restrict file imports to the import folder

References

Release notes

Credits

We want to publicly recognise the contribution of Yotam Perkal from Pluto Security.

Severity

Low 2.3 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	Present
Privileges Required	Low
User interaction	None
Vulnerable System Impact Metrics	
Confidentiality	Low
Integrity	Low
Availability	None
Subsequent System Impact Metrics	
Confidentiality	Low
Integrity	Low
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N

CVE ID

CVE-2026-35402

Weaknesses

▶ CWE-284

Credits

 **yotampe-pluto** Reporter