



CVE-2018-1000820

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-1000820
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-20 15:29:00 UTC
Updated	2023-01-23 15:40:00 UTC
Description	neo4j-contrib neo4j-apoc-procedures version before commit 45bc09c contains a XML External Entity (XXE) vulnerability in

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Neo4j	Awesome Procedures On Cyper	All	All	All	All
Application	Neo4j-contrib	Neo4j-apoc-procedures	All	All	All	All
Application	Neo4j-contrib	Neo4j-apoc-procedures	All	All	All	All

References

Reference	Source	Link	Tags
Neo4j Apoc Procedures XXE Odd - The Zero (0) Day Division	MISC	Odd.zone	Third Party Advisory
XXE in Xml.java · Issue #931 · neo4j-contrib/neo4j-apoc-procedures · GitHub	MISC	github.com	Issue Tracking, Patch, Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

982319 Java (maven) Security Update for org.neo4j.procedure:apoc (GHSA-r2pp-x4mm-4999)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)