



CVE-2023-45960

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-45960
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-25 18:17:00 UTC
Updated	2023-11-07 04:21:00 UTC
Description	** DISPUTED ** An issue in dom4j.org.dom4.io.SAXReader v.2.1.4 and before allows a remote attacker to obtain sensitive

Risk And Classification

Problem Types: CWE-91

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dom4j Project	Dom4j	All	All	All	All

References

Reference	Source	Link
works only up to v2.1.0 · Issue #1 · joker-xiaoyan/XXE-SAXReader · GitHub	MISC	github.com
GitHub - joker-xiaoyan/XXE-SAXReader	MISC	github.com
according to some vulnerability databases, dom4j is affected by CVE-2023-45960 · Issue #171 · dom4j/dom4j · GitHub	MISC	github.com
dom4j	MISC	dom4j.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

995759 Java (Maven) Security Update for org.dom4j:dom4j (GHSA-fgq9-fc3q-vqmw)

© [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](#)