



xmldom: Denial of service via uncontrolled recursion in XML serialization

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

Summary

CVE	CVE-2026-41673
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-07 04:16:33 UTC
Updated	2026-05-07 15:16:08 UTC

Description xmldom is a pure JavaScript W3C standard-based (XML DOM Level 2 Core) `DOMParser` and `XMLSerializer` module. In

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000810000 probability, percentile 0.236160000 (date 2026-05-12)

Problem Types: CWE-674 | CWE-674 CWE-674: Uncontrolled Recursion

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Xmldom	Xmldom	affected xmldom <= 0.6.0	Not specified
CNA	Xmldom	Xmldom	affected @xmldom/xmldom >= 0.9.0, < 0.9.10	Not specified
CNA	Xmldom	Xmldom	affected @xmldom/xmldom < 0.8.13	Not specified

References

Reference	Source	Link
github.com/xmldom/xmldom/commit/291257493cb0eb6980eda83b162a9c4e6d7d2597	security-advisories@github.com	github.c
github.com/xmldom/xmldom/security/advisories/GHSA-2v35-w6hq-6mfw	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.c
github.com/xmldom/xmldom/commit/4845ef109221df0890825de2822f77afba3afe	security-advisories@github.com	github.c
github.com/xmldom/xmldom/commit/2d6d6916ed8a4c223db1f6d7560ab4544c465b0f	security-advisories@github.com	github.c
github.com/xmldom/xmldom/commit/430357c7b6333108856e917bf2367afe5ceb6f8a	security-advisories@github.com	github.c
github.com/xmldom/xmldom/releases/tag/0.9.10	security-advisories@github.com	github.c
github.com/xmldom/xmldom/commit/b0620383abc1df067f3ce1014c43ae1bc1161eeb	security-advisories@github.com	github.c
github.com/xmldom/xmldom/commit/8b7cfd1491314abdc347261921d7334ff15f7112	security-advisories@github.com	github.c
github.com/xmldom/xmldom/commit/8834218c85ac2a4d757b9587c9028e67c2f7b6c3	security-advisories@github.com	github.c
github.com/xmldom/xmldom/commit/17678a2a73ecbd1a2da90f3d47dc23da9cef81aa	security-advisories@github.com	github.c
github.com/xmldom/xmldom/commit/e6edcab6bef5bcdba0b220bb35442aa72f452b84	security-advisories@github.com	github.c
github.com/xmldom/xmldom/releases/tag/0.8.13	security-advisories@github.com	github.c
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)