



xmldom: XML node injection through unvalidated comment serialization

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

Summary

CVE	CVE-2026-41672
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 16:16:20 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:H/VA:N/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: 0.000560000 probability, percentile 0.175040000 (date 2026-05-12)

Problem Types: CWE-91 | CWE-91 CWE-91: XML Injection (aka Blind XPath Injection)

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:H/VA:N/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:H/VA:N/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

High

Availability

None

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:H/VA:N/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/b397540889086da868c30c366ad5c220d1a750c7	security-advisories@github.com	github.com
github.com/xmldom/xmldom/pull/987	security-advisories@github.com	github.com
github.com/xmldom/xmldom/commit/fda7cc313de30243fea35cada64e0bb12099c2a1	security-advisories@github.com	github.com
github.com/xmldom/xmldom/security/advisories/GHSA-j759-j44w-7fr8	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
github.com/xmldom/xmldom/releases/tag/0.9.10	security-advisories@github.com	github.com
github.com/xmldom/xmldom/releases/tag/0.8.13	security-advisories@github.com	github.com
CVE Program record	CVE.ORG	www.cve
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.

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