



# DOMPurify: Prototype Pollution to XSS Bypass via CUSTOM\_ELEMENT\_HANDLING Fallback

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

## Summary

<b>CVE</b>	CVE-2026-41238
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-23 16:16:26 UTC
<b>Updated</b>	2026-04-23 18:16:29 UTC
<b>Description</b>	DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Versions 3.0.1 through 3.3.3 are vuln

## Risk And Classification

**Primary CVSS:** v3.1 6.9 MEDIUM from security-advisories@github.com

**CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:L/A:N**

**Problem Types:** CWE-79 | CWE-1321 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | CWE-1321 CWE-1321: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	6.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:L/A:N
3.1	CNA	DECLARED	6.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**High**

Privileges Required

**None**

User Interaction

**Required**

Scope

**Changed**

Confidentiality

**High**

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:L/A:N

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cure53	DOMPurify	affected >= 3.0.1, < 3.4.0	Not specified

### References

Reference	Source	Link	Tags
github.com/cure53/DOMPurify/releases/tag/3.4.0	security-advisories@github.com	github.com	
github.com/cure53/DOMPurify/security/advisories/GHSA-v9jr-rg53-9pgp	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)