



# SandboxJS: Sandbox integrity escape

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

## Summary

<b>CVE</b>	CVE-2026-34208
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-06 16:16:34 UTC
<b>Updated</b>	2026-04-09 18:07:20 UTC
<b>Description</b>	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.36, SandboxJS blocks direct assignment to global objects (for e)

## Risk And Classification

**Primary CVSS:** v3.1 10 CRITICAL from nvd@nist.gov

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

**EPSS:** 0.000600000 probability, percentile 0.187170000 (date 2026-04-07)

**Problem Types:** CWE-693 | CWE-915 | CWE-693 CWE-693: Protection Mechanism Failure | CWE-915 CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	security-advisories@github.com	Secondary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L
3.1	CNA	DECLARED	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nyariv	Sandboxjs	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Nyariv	SandboxJS	affected < 0.8.36	Not specified

### References

Reference	Source	Link	Tags
github.com/nyariv/SandboxJS/security/advisories/GHSA-2gg9-6p7w-6cpj	security-advisories@github.com	github.com	Exploit, Vendor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

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