Bug 2312579 (CVE-2024-11831) - CVE-2024-11831 npm-serialize-javascript: Cross-site Scripting (XSS) in serialize-javascript

Keywords: Security

Status: NEW

Alias: CVE-2024-11831

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2312824 2312604 ~~2312608~~ ~~2312609~~ ~~2312610~~ ~~2312611~~ ~~2312612~~ ~~2312613~~ ~~2312614~~ ~~2312615~~ ~~2312616~~ ~~2312617~~ ~~2312618~~ ~~2312619~~ ~~2312620~~ ~~2312621~~ ~~2312622~~ 2389951 2389952 2389953 2389954 2389955 2389956 2389957 2389959 2393368 2393369 2393371 2393373

Blocks:

TreeView+ depends on / blocked

Reported: 2024-09-16 17:03 UTC by OSIDB Bzimport

Modified: 2026-04-01 08:28 UTC (History)

CC List: 221 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat	RHSA-2025:1334	0	None	None	None	2025-02-11

Product Errata						21:20:43 UTC
Red Hat Product Errata	RHSA-2025:1468	0	None	None	None	2025-02-13 18:15:09 UTC
Red Hat Product Errata	RHSA-2025:4511	0	None	None	None	2025-05-06 07:15:18 UTC
Red Hat Product Errata	RHSA-2025:8479	0	None	None	None	2025-06-04 01:59:25 UTC
Red Hat Product Errata	RHSA-2025:8544	0	None	None	None	2025-06-04 20:12:22 UTC
Red Hat Product Errata	RHSA-2025:8551	0	None	None	None	2025-06-04 22:59:33 UTC
Red Hat Product Errata	RHSA-2026:1536	0	None	None	None	2026-01-29 06:52:18 UTC
Red Hat Product Errata	RHSA-2026:2769	0	None	None	None	2026-02-17 00:50:59 UTC

OSIDB Bzimport 2024-09-16 17:03:58 UTC Description

```
The serialize-javascript module is vulnerable to Cross-Site
Scripting (XSS) due to insufficient sanitization of serialized
JavaScript objects, specifically affecting versions before
6.0.2. Attackers can inject malicious scripts that could
execute in the context of the user's browser, leading to
unauthorized actions or data exposure.
```

errata-xmlrpc 2025-02-11 21:20:32 UTC Comment 7

```
This issue has been addressed in the following products:

  Red Hat Advanced Cluster Security 4.5

Via RHSA-2025:1334 https://access.redhat.com/errata/RHSA-
2025:1334
```

errata-xmlrpc 2025-02-13 18:14:57 UTC Comment 8

This issue has been addressed in the following products:

  Red Hat Advanced Cluster Security 4.4

Via RHSA-2025:1468 https://access.redhat.com/errata/RHSA-2025:1468

errata-xmlrpc 2025-05-06 07:15:03 UTC Comment 14

This issue has been addressed in the following products:

  RHODF-4.18-RHEL-9

Via RHSA-2025:4511 https://access.redhat.com/errata/RHSA-2025:4511

errata-xmlrpc 2025-06-04 01:59:11 UTC Comment 18

This issue has been addressed in the following products:

  RHODF-4.16-RHEL-9

Via RHSA-2025:8479 https://access.redhat.com/errata/RHSA-2025:8479

errata-xmlrpc 2025-06-04 20:12:10 UTC Comment 19

This issue has been addressed in the following products:

  RHODF-4.15-RHEL-9

Via RHSA-2025:8544 https://access.redhat.com/errata/RHSA-2025:8544

errata-xmlrpc 2025-06-04 22:59:19 UTC Comment 20

This issue has been addressed in the following products:

  RHODF-4.14-RHEL-9

Via RHSA-2025:8551 https://access.redhat.com/errata/RHSA-

2025:8551

errata-xmlrpc 2026-01-29 06:52:03 UTC Comment 25

This issue has been addressed in the following products:

Red Hat Ceph Storage 9.0

Via RHSA-2026:1536 https://access.redhat.com/errata/RHSA-2026:1536

errata-xmlrpc 2026-02-17 00:50:44 UTC Comment 27

This issue has been addressed in the following products:

Red Hat Ceph Storage 7.1

Via RHSA-2026:2769 https://access.redhat.com/errata/RHSA-2026:2769

Note

You need to log in before you can comment on or make changes to this bug.