



CVE-2023-28445

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

Summary

CVE	CVE-2023-28445
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-24 00:15:00 UTC
Updated	2023-03-31 13:07:00 UTC
Description	Deno is a runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Resizable ArrayBuffers passed to asynch

Risk And Classification

Problem Types: CWE-125 | CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Deno	Deno	1.32.0	All	All	All
Application	Deno	Deno Runtime	0.102.0	All	All	All
Application	Deno	Serde V8	0.87.0	All	All	All

References

Reference	Source
Improper handling of resizable ArrayBuffer in async built-in functions · Advisory · denoland/deno · GitHub	MISC
Release v1.32.1 · denoland/deno · GitHub	MISC
core: disable resizable ArrayBuffer and growable SharedArrayBuffer by bartlomieju · Pull Request #18395 · denoland/deno · GitHub	MISC
CVE Program record	CVE.O
NVD vulnerability detail	NVD

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](#)