



CVE-2023-44769

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

Summary

CVE	CVE-2023-44769
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-25 18:17:00 UTC
Updated	2023-11-01 16:15:00 UTC
Description	A Cross-Site Scripting (XSS) vulnerability in Zenario CMS v.9.4.59197 allows a local attacker to execute arbitrary code via a

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tribalsystems	Zenario	9.4.59197	All	All	All

References

Reference

- [GitHub - sromanhu/CVE-2023-44769_ZenarioCMS--Reflected-XSS---Alias: Zenariocms 9.4.59197 is affected by a Cross-Site Scripting \(XSS\)](#)
- [GitHub - sromanhu/CVE-2023-44769_ZenarioCMS--Reflected-XSS---Alias: Zenariocms 9.4.59197 is affected by a Cross-Site Scripting \(XSS\)](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995808](#) PHP (Composer) Security Update for tribalsystems/zenario (GHSA-8g87-73vq-443p)

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