



# CVE-2023-44771

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-44771
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-10-06 13:15:00 UTC
<b>Updated</b>	2023-10-06 19:06:00 UTC
<b>Description</b>	A Cross-Site Scripting (XSS) vulnerability in Zenario CMS v.9.4.59197 allows a local attacker to execute arbitrary code via c

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Tribalsystems</a>	<a href="#">Zenario</a>	9.4.59197	All	All	All

## References

Reference
<a href="#">GitHub - sromanhu/ZenarioCMS--Stored-XSS---Page-Layout: Zenariocms 9.4.59197 is affected by a Cross-Site Scripting (XSS) vulnerability t</a>
<a href="#">CVE Program record</a>
<a href="#">NVD vulnerability detail</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[995531](#) PHP (Composer) Security Update for tribalsystems/zenario (GHSAs-6cxv-27r2-fp3m)

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)