



CVE-2023-36492

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

Summary

CVE	CVE-2023-36492
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-05 10:15:00 UTC
Updated	2023-09-08 16:48:00 UTC
Description	Reflected cross-site scripting vulnerability in SHIRASAGI prior to v1.18.0 allows a remote unauthenticated attacker to execute arbitrary JavaScript code.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ss-proj	Shirasagi	All	All	All	All

References

Reference	Source	Link
JVN#82758000: Multiple vulnerabilities in SHIRASAGI	MISC	jvn.jp
SHIRASAGI におけるクロスサイト・スクリプティング脆弱性とバストラバーサル脆弱性 - SHIRASAGI公式サイト	MISC	www.ss-proj.org/shirasagi/
CVE Program record	CVE.ORG	www.cve.org/CVE.experts/CVE-2023-36492
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2023-36492

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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