CVE-2022-34007

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-34007
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-07 12:15:00 UTC
Updated	2022-10-26 22:28:00 UTC
Description	EQS Integrity Line Professional through 2022-07-01 allows a stored XSS via a crafted whistleblower entry.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eqs	Integrity Line	All	All	All	All
Application	Eqs	Integrity Line	All	All	All	All

References

Reference	Source	Link
www.ush.it/team/ush/advisory-eqs-integrity-line/eqs_integrity_line.txt	MISC	www.ush.it
The Pitfalls of Closed-Source Whistleblowing Software - Whistleblowing International Network	MISC	whistleblowingnetwork.org
Full Disclosure: EQS Integrity Line: Multiple Vulnerabilities	MISC	seclists.org
EQS Integrity Line - the secure whistleblowing hotline | integrityline.com	MISC	www.integrityline.com
EQS Integrity Line Cross Site Scripting / Information Disclosure ≈ Packet Storm	MISC	packetstormsecurity.com
Compliance	MISC	eusanctions.integrityline.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report