CVE-2020-15716

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

Summary

CVE	CVE-2020-15716
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-15 19:15:00 UTC
Updated	2020-07-22 16:59:00 UTC
Description	RosarioSIS 6.7.2 is vulnerable to XSS, caused by improper validation of user-supplied input by the Preferences.php script.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rosariosis	Rosariosis	6.7.2	All	All	All
Application	Rosariosis	Rosariosis	6.7.2	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	MISC	exchange.xfor
Fix #291 XSS Use URLEscape() for forms action (89ae9de7) · Commits · François Jacquet / rosariosis · GitLab	CONFIRM	gitlab.com
v6.8-beta · Tags · François Jacquet / rosariosis · GitLab	MISC	gitlab.com
Reflected Cross-Site Scripting in different locations (#291) · Issues · François Jacquet / rosariosis · GitLab	MISC	gitlab.com
CHANGES.md · mobile · François Jacquet / rosariosis · GitLab	MISC	gitlab.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