



# CVE-2021-44566

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

## Summary

<b>CVE</b>	CVE-2021-44566
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-02-24 15:15:00 UTC
<b>Updated</b>	2022-03-03 03:14:00 UTC
<b>Description</b>	A Cross Site Scripting (XSS) vulnerability exists in RosarioSIS before 4.3 via the SanitizeMarkdown function in ProgramFu

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source
CHANGES_V3_4.md · mobile · François Jacquet / rosariosis · GitLab	MISC
Fix #259 Prevent XSS: Sanitize the newly created Markdown text (81886abb) · Commits · François Jacquet / rosariosis · GitLab	MISC
Stored XSS Vulnerability (#259) · Issues · François Jacquet / rosariosis · GitLab	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)