



# CVE-2022-2036

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

## Summary

<b>CVE</b>	CVE-2022-2036
<b>State</b>	PUBLIC
<b>Assigner</b>	security@huntr.dev
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-06-09 17:15:00 UTC
<b>Updated</b>	2022-06-15 18:27:00 UTC
<b>Description</b>	Cross-site Scripting (XSS) - Stored in GitHub repository francoisjacquet/rosariosis prior to 9.0.1.

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link
Bypass filter - Stored XSS in Resources vulnerability found in rosariosis	CONFIRM	<a href="#">huntr.dev</a>
Fix stored XSS security issue: decode HTML entities from URL - francoisjacquet/rosariosis@6e213b1 - GitHub	MISC	<a href="#">github.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

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

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