



CVE-2021-44567

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

Summary

CVE	CVE-2021-44567
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-24 15:15:00 UTC
Updated	2022-03-03 03:58:00 UTC
Description	An unauthenticated SQL Injection vulnerability exists in RosarioSIS before 7.6.1 via the votes parameter in ProgramFuncio

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

- Unauthenticated SQL Injection in /ProgramFunctions/PortalPollsNotes.fnc.php Due to Insufficient Sanitization (#308) · Issues · François Jacqu
- Fix #308 Unauthenticated SQL injection. Use sanitized `\$_REQUEST` + Move... (e001430a) · Commits · François Jacquet / rosariosis · GitLab
- CHANGES.md · mobile · François Jacquet / rosariosis · GitLab
- Fix #308 security issue sanitize key. Pass array keys through function (519af055) · Commits · François Jacquet / rosariosis · GitLab
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)