

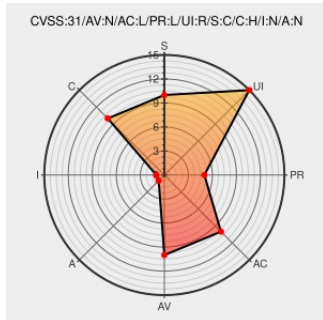


CVE-2021-21319

Published on: 10/25/2021 12:00:00 AM UTC

Last Modified on: 10/28/2021 01:12:00 AM UTC

CVE-2021-21319 - advisory for GHSA-vjc9-mj44-x59q

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Galette](#) from [Galette](#) contain the following vulnerability:

Galette is a membership management web application geared towards non profit organizations. In versions prior to 0.9.5, malicious javascript code can be stored to be displayed later on self subscription page. The self subscription feature can be disabled as a workaround (this is the default state). Malicious javascript code can be executed (not stored) on login and retrieve password pages. This issue is patched in version 0.9.5.

CVE-2021-21319 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **galette** - **galette** version < 0.9.5

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
-------------	------	------

Description	Tags	Link
Prevent some possible XSS · gallette/galette@514418d · GitHub	github.com text/html	MISC github.com/galette/galette/commit/514418da973ae5b84bf97f94bd288a41e8e3f0a6
Galette bugs & features	bugs.galette.eu text/html	MISC bugs.galette.eu/issues/1535
Fix stored XSS on dynamic fields configuration · gallette/galette@8f3bdd9 · GitHub	github.com text/html	MISC github.com/galette/galette/commit/8f3bdd9f7d0708466e011253064a867ca2b271a5
Several stored XSS · Advisory · gallette/galette · GitHub	github.com text/html	CONFIRM github.com/galette/galette/security/advisories/GHSA-vjc9-mj44-x59q
Add test on stored xss · gallette/galette@f54b257 · GitHub	github.com text/html	MISC github.com/galette/galette/commit/f54b2570615d38d0302e937079233e52c2d80995

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Galette	Galette	All	All	All	All
cpe:2.3:a:galette:galette:*:*:*:*:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-21319 : Galette is a membership management web application geared towards non profit organizations. In ver... twitter.com/i/web/status/1...	2021-10-25 16:03:39

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

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