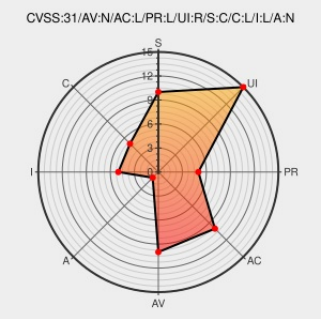
CVE-2021-41142

Published on: 10/14/2021 12:00:00 AM UTC

Last Modified on: 10/20/2021 06:07:00 PM UTC

CVE-2021-41142 - advisory for GHSA-p3j6-6h9h-34r5

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Tuleap from Enalean contain the following vulnerability:

Tuleap Open ALM is a libre and open source tool for end to end traceability of application and system developments. There is a cross-site scripting vulnerability in Tuleap Community Edition prior to 12.11.99.25 and Tuleap Enterprise Edition 12.11-2. A malicious user with the capability to add and remove attachment to an artifact could force a victim to execute uncontrolled code. Tuleap Community Edition 11.17.99.146 and Tuleap Enterprise Edition 12.11-2 contain a fix for the issue.

CVE-2021-41142 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Enalean** - **tuleap** version **< 12.11.99.25**

Affected Vendor/Software: **Enalean** - **tuleap** version **>= 12.11-1, < 12.11-2**

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
XSS via the name of a deleted attachment - request #22570 - Requests - Tuleap	tuleap.net text/html	MISC tuleap.net/plugins/tracker/?aid=22570
Git - Tuleap	tuleap.net text/html	MISC tuleap.net/plugins/git/tuleap/tuleap/stable?a=commit&h=d6c837ed6fa66d319175954a42f93d4d86745208
request #22570: XSS via the name of a deleted attachment · Enalean/tuleap@d6c837e · GitHub	github.com text/html	MISC github.com/Enalean/tuleap/commit/d6c837ed6fa66d319175954a42f93d4d86745208
XSS via the name of a deleted attachment · Advisory · Enalean/tuleap · GitHub	github.com text/html	CONFIRM github.com/Enalean/tuleap/security/advisories/GHSA-p3j6-6h9h-34r5

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Enalean	Tuleap	All	All	All	All
Application	Enalean	Tuleap	All	All	All	All

cpe:2.3:a:enalean:tuleap:*:*:*:*:community:*:*:*:

cpe:2.3:a:enalean:tuleap:*:*:*:*:enterprise:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41142 : Tuleap Open ALM is a libre and open source tool for end to end traceability of application and sys… twitter.com/i/web/status/1…	2021-10-14 16:10:30

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report