



CVE-2021-24487

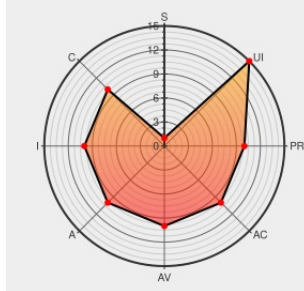
Published on: 10/25/2021 12:00:00 AM UTC

Last Modified on: 02/15/2023 02:30:00 AM UTC

CVE-2021-24487

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

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [St-daily-tip](#) from [Sanskriti](#) contain the following vulnerability:

The St-Daily-Tip WordPress plugin through 4.7 does not have any CSRF check in place when saving its 'Default Text to Display if no tips' setting, and was also lacking sanitisation as well as escaping before outputting it the page. This could allow attacker to make logged in administrators set a malicious payload in it, leading to a Stored Cross-Site Scripting issue

CVE-2021-24487 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Unknown - St-Daily-Tip** version <= 4.7

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

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



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

Exploit/POC from Github

The St-Daily-Tip WordPress plugin through 4.7 does not have any CSRF check in place when saving its 'Default Text to ...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sanskriti	St-daily-tip	All	All	All	All
cpe:2.3:a:sanskriti:st-daily-tip:*:*:*:*:wordpress:*:*:						

Discovery Credit

Akash Rajendra Patil

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-24487 : The St-Daily-Tip WordPress plugin through 4.7 does not have any CSRF check in place when saving it... twitter.com/i/web/status/1...	2021-10-25 13:28:35
@LinInfoSec	Wordpress - CVE-2021-24487: wpscan.com/vulnerability/...	2021-10-25 16:50:31

[← Previous ID](#)

[Next ID →](#)