VDB-355414 · CVE-2026-5624 · GCVE-100-355414

PROJECTSEND R2002 UPLOAD.PHP CROSS-SITE REQUEST FORGERY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.9	$0-$5k	2.01-

Summary

A vulnerability labeled as problematic has been found in ProjectSend r2002. This issue affects some unknown processing of the file *upload.php*. Executing a manipulation can lead to cross-site request forgery. The identification of this vulnerability is CVE-2026-5624. The attack may be launched remotely. Furthermore, there is an exploit available. The affected component should be upgraded.

Details

A vulnerability has been found in ProjectSend r2002 and classified as problematic. This vulnerability affects an unknown part of the file *upload.php*. The manipulation with an unknown input leads to a cross-site request forgery vulnerability. The CWE definition for the vulnerability is CWE-352. The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request. As an impact it is known to affect integrity.

This vulnerability was named CVE-2026-5624. The exploitation appears to be easy. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Successful exploitation requires user interaction by the victim. Technical details and also a public exploit are known.

It is declared as proof-of-concept. By approaching the search of inurl:upload.php it is possible to find vulnerable targets with Google Hacking.

Upgrading to version r2029 eliminates this vulnerability. The upgrade is hosted for download at github.com. Applying the patch 2c0d25824ab571b6c219ac1a188ad9350149661b is able to eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.

Product

Type

- Project Management Software

Name

- ProjectSend

Version

- r2002

License

- open-source

Website

- Product: https://github.com/projectsend/projectsend/

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 4.3
VulDB Meta Temp Score: 3.9

VulDB Base Score: 4.3
VulDB Temp Score: 3.9
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Cross-site request forgery
CWE: CWE-352 / CWE-862 / CWE-863
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Google Hack: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: Upgrade
Status: 🔍

0-Day Time: 🔒

Upgrade: ProjectSend r2029
Patch: 2c0d25824ab571b6c219ac1a188ad9350149661b

Timeline

04/05/2026		Advisory disclosed
04/05/2026	+0 days	VulDB entry created
04/05/2026	+0 days	VulDB entry last update

Sources

Product: github.com

Status: Confirmed

CVE: CVE-2026-5624 (🔒)
GCVE (CVE): GCVE-0-2026-5624
GCVE (VulDB): GCVE-100-355414
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/05/2026 06:56 PM
Changes: 04/05/2026 06:56 PM (58)
Complete: 🔍
Submitter: AquaNight
Cache ID: 172:67E:179

Submit

Accepted

- Submit #785731: ProjectSend projectsend r2002 Cross-Site Request Forgery (by AquaNight)

Discussion

No comments yet. Languages: en.

Please log in to comment.