VDB-355406 · CVE-2026-5615 · GCVE-100-355406

GIVANZ VVVEBJS UP TO 2.0.5 FILE UPLOAD ENDPOINT UPLOAD.PHP UPLOADALLOWEXTENSIONS CROSS SITE SCRIPTING

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.9	$0-$5k	1.99-

Summary

A vulnerability, which was classified as problematic, was found in givanz Vvvebjs up to 2.0.5. The impacted element is an unknown function of the file *upload.php* of the component *File Upload Endpoint*. Such manipulation of the argument *uploadAllowExtensions* leads to cross site scripting. This vulnerability is documented as CVE-2026-5615. The attack can be executed remotely. Additionally, an exploit exists. It is best practice to apply a patch to resolve this issue. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.

Details

A vulnerability was found in givanz Vvvebjs up to 2.0.5 and classified as problematic. Affected by this issue is some unknown functionality of the file *upload.php* of the component *File Upload Endpoint*. The manipulation of the argument `uploadAllowExtensions` with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-79. The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. Impacted is integrity.

The advisory is available at tcn60zf28jhk.feishu.cn. This vulnerability is handled as CVE-2026-5615. The exploitation is known to be easy. The attack may be launched remotely. No form of authentication is required for exploitation. Successful exploitation requires user interaction by the victim. Technical details as well as a public exploit are known. This vulnerability is assigned to T1059.007 by the MITRE ATT&CK project.

The exploit is available at tcn60zf28jhk.feishu.cn. It is declared as proof-of-concept. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product. By approaching the search of inurl:upload.php it is possible to find vulnerable targets with Google Hacking.

Applying the patch 8cac22cff99b8bc701c408aa8e887fa702755336 is able to eliminate this problem. The bugfix is ready for download at github.com.

Entries connected to this vulnerability are available at VDB-271667, VDB-316959, VDB-317690 and VDB-318422.

Product

Vendor

- givanz

Name

- Vvvebjs

Version

- 2.0.0
- 2.0.1
- 2.0.2
- 2.0.3
- 2.0.4
- 2.0.5

License

- open-source

Website

- Product: https://github.com/givanz/VvvebJs/

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 scripting
CWE: CWE-79 / CWE-94 / CWE-74
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

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

Threat Intelligence

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

Countermeasures

Recommended: Patch
Status: 🔍

0-Day Time: 🔒

Patch: 8cac22cff99b8bc701c408aa8e887fa702755336

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

Advisory: tcn60zf28jhk.feishu.cn
Status: Confirmed

CVE: CVE-2026-5615 (🔒)
GCVE (CVE): GCVE-0-2026-5615
GCVE (VulDB): GCVE-100-355406
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/05/2026 05:37 PM
Changes: 04/05/2026 05:37 PM (61)
Complete: 🔍

Submitter: EthX0_
Cache ID: 20:F91:179

Submit

Accepted

- Submit #785563: givanz VvvebJs 2.0.5 Stored XSS (by EthX0_)

Discussion

No comments yet. Languages: en.

Please log in to comment.