



givanz Vvweb Drag-and-Drop Editor editor server-side request forgery

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2025-8520
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-08-04 18:15:36 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability classified as critical was found in givanz Vvweb up to 1.0.5. This vulnerability affects unknown code of the file

Risk And Classification

Primary CVSS: v4.0 2 LOW from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-918 | CWE-918 Server-Side Request Forgery

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	2	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Secondary	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	4.7	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	5.8		AV:N/AC:L/Au:M/C:P/I:P/A:P
2.0	CNA	DECLARED	5.8		AV:N/AC:L/Au:M/C:P/I:P/A:P/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Vvweb	Vvweb	All	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Givanz	Vvweb	affected 1.0.0	Not specified		
CNA	Givanz	Vvweb	affected 1.0.1	Not specified		
CNA	Givanz	Vvweb	affected 1.0.2	Not specified		
CNA	Givanz	Vvweb	affected 1.0.3	Not specified		
CNA	Givanz	Vvweb	affected 1.0.4	Not specified		
CNA	Givanz	Vvweb	affected 1.0.5	Not specified		
CNA	Givanz	Vvweb	unaffected 1.0.6	Not specified		
References						
Reference	Source			Link		
vuldb.com	134c704f-9b21-4f2e-91b3-4a467353bcc0			vuldb.com		
github.com/givanz/Vvweb/commit/f684f3e374d04db715730fc4796e102f5ebcacb2	cna@vuldb.com			github.com		
github.com/givanz/Vvweb/releases/tag/1.0.6	cna@vuldb.com			github.com		
vuldb.com	cna@vuldb.com			vuldb.com		
vuldb.com	cna@vuldb.com			vuldb.com		
hkohi.ca/vulnerability/9	134c704f-9b21-4f2e-91b3-4a467353bcc0			hkohi.ca		
CVE Program record	CVE.ORG			www.cve.org		

NVD vulnerability detailNVDnvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: 0xHamy (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-08-04T00:00:00.000Z	Advisory disclosed
CNA	2025-08-04T02:00:00.000Z	VulDB entry created
CNA	2025-08-04T08:32:19.000Z	VulDB entry last update

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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