Vvveb < 1.0.8.3 Stored XSS via Signup Controller

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-41932
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-14 15:16:45 UTC
Updated	2026-05-14 15:16:45 UTC
Description	Vvveb before 1.0.8.3 contains a stored cross-site scripting vulnerability in the customer signup flow where the Signup::addU

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from disclosure@vulncheck.com

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

Problem Types: CWE-79 | CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:L/SI:L/SA
4.0	CNA	CVSS	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:L/SI:L/SA
3.1	disclosure@vulncheck.com	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC: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

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Givanz	Vvveb	affected 1.0.8.3 semver	Not specified
CNA	Givanz	Vvveb	unaffected fefac290a8c85d3c87fe80ffed68b6c5bc50e93c git	Not specified

References

Reference	Source	Link	Tags

www.vulncheck.com/advisories/vvveb-stored-xss-via-signup-controller	disclosure@vulncheck.com	www.vulncheck.com	
github.com/givanz/Vvveb/commit/fefac290a8c85d3c87fe80ffed68b6c5bc50e93c	disclosure@vulncheck.com	github.com	
github.com/givanz/Vvveb/releases/tag/1.0.8.3	disclosure@vulncheck.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

Vendor Comments And Credit

Discovery Credit

CNA: Basant Kumar (@CyberWarrior9) (en)

CNA: VulnCheck (en)

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