



WordPress Plugin AccessPress Social Icons 1.8.2

Stored XSS

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2021-47910
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-10 13:16:27 UTC
Updated	2026-05-12 14:24:15 UTC
Description	AccessPress Social Icons 1.8.2 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inje

Risk And Classification

Primary CVSS: v4.0 5.1 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000300000 probability, percentile 0.088110000 (date 2026-05-12)

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	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA
3.1	disclosure@vulncheck.com	Primary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Passive

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/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/MSX: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

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Accesspressthemes	AccessPress Social Icons	affected 1.8.2	Not specified

References

Reference	Source	Link
accesspressthemes.com	disclosure@vulncheck.com	accesspressthemes.co
wordpress.org/plugins/accesspress-social-icons	disclosure@vulncheck.com	wordpress.org
www.exploit-db.com/exploits/50515	disclosure@vulncheck.com	www.exploit-db.com
www.vulncheck.com/advisories/wordpress-plugin-accesspress-social-icons-stored-xss	disclosure@vulncheck.com	www.vulncheck.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit
CNA: Murat DEMIRCI (@butterflyhunt3r) (en)

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