



WordPress WP CleanFix plugin <= 5.6.2 - Broken Access Control vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2023-48775
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-31 13:15:05 UTC
Updated	2026-04-28 19:22:16 UTC
Description	Missing Authorization vulnerability in Gfazioli WP Cleanfix allows Exploiting Incorrectly Configured Access Control Security

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from audit@patchstack.com

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

EPSS: 0.001330000 probability, percentile 0.325580000 (date 2026-04-28)

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Gfazioli	WP Cleanfix	affected n/a 5.6.2 custom	Not specified

References

Reference

patchstack.com/database/wordpress/plugin/wp-cleanfix/vulnerability/wordpress...

https://patchstack.com/database/wordpress/plugin/wp-cleanfix/vulnerability/wordpress-wp-cleanfix-plugin-5-5-0-broken-access-control-vulnera

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: Abdi Pranata (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: No patched version is available. No reply from the vendor.

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