



WordPress RestoPress plugin <= 3.2.3.5 - Broken Access Control vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2025-66100
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-18 08:16:15 UTC
Updated	2026-04-28 22:16:28 UTC
Description	Missing Authorization vulnerability in Magnigenie RestoPress restopress allows Exploiting Incorrectly Configured Access C

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from audit@patchstack.com

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

EPSS: 0.000510000 probability, percentile 0.159020000 (date 2026-04-28)

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

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Magnigenie	RestroPress	affected 3.2.3.5 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/restropress/vulnerability/wordpress...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

Vendor Comments And Credit

Discovery Credit

CNA: daroo | Patchstack Bug Bounty Program (en)

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