WordPress Cloak Front End Email <= 1.9.5 - Broken Access Control Vulnerability

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

Summary

CVE	CVE-2025-26968
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-17 16:15:34 UTC
Updated	2026-04-28 19:29:52 UTC
Description	Missing Authorization vulnerability in webbernaut Cloak Front End Email allows Exploiting Incorrectly Configured Access Co

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from audit@patchstack.com

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

EPSS: 0.002290000 probability, percentile 0.455630000 (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	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Webbernaut	Cloak Front End Email	affected n/a 1.9.5 custom	Not specified

References

Reference
patchstack.com/database/wordpress/plugin/cloak-front-end-email/vulnerability...
https://patchstack.com/database/wordpress/plugin/cloak-front-end-email/vulnerability/wordpress-cloak-front-end-email-1-9-5-broken-access-cc
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: muhammad yudha (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update the WordPress Cloak Front End Email plugin to the latest available version (at least 1.9.6).

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