An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2608250238

NCSC Advisory

Critical Vulnerability exists in Wordpress Plugin: Pods – Custom Content Types and Fields

CVE-2026-19598

25th, August 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-19598

Published: 2026-08-15

Vendor: sc0ttkclark

Product: Pods – Custom Content Types and Fields

CVSS Score[1]: 9.8

Products Affected

Product	Version
Pods – Custom Content Types and Fields	2.8 <= 2.8.23.3
Pods – Custom Content Types and Fields	2.9 <= 2.9.19.3
Pods – Custom Content Types and Fields	3.0 <= 3.0.10.3
Pods – Custom Content Types and Fields	3.1 <= 3.1.4.1
Pods – Custom Content Types and Fields	3.2 <= 3.2.8.2
Pods – Custom Content Types and Fields	3.3 <= 3.3.9

Impact

The Pods – Custom Content Types and Fields plugin for WordPress is vulnerable to Privilege Escalation via Authorization Bypass in all versions up to, and including, 3.3.9.

The vulnerability exists because the pods_admin AJAX router funnels every access check — including the method allowlist, nonce verification, login enforcement, and capability gate — through pods_error(), which under the JSON meta-box-loader compatibility path only writes failures to the PHP error log and returns false instead of terminating the request, rendering all guards ineffective.

This makes it possible for unauthenticated attackers to escalate their privileges to Administrator or overwrite the password of any user account, including the site owner's, enabling complete site takeover, or perform another administrator action.,

[1] https://www.first.org/cvss/

Common Weakness Enumeration (CWE)[2]: CWE-863: Incorrect Authorization

Actively Exploited Vulnerability: Yes[3]

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from sc0ttkclark.

- https://nvd.nist.gov/vuln/detail/CVE-2026-19598
- https://www.cve.org/CVERecord?id=CVE-2026-19598
- https://www.wordfence.com/threat-intel/vulnerabilities/id/3628032a-3121-45a7-8a78-cfcd8ba6af2f?source=cve
- https://plugins.trac.wordpress.org/browser/pods/tags/3.3.9/includes/general.php#L400

[2] https://cwe.mitre.org
[3] https://previdian.com/CVE-2026-19598