NATIONAL CSIRT-CY

CVE-2025-3418

13/04/2025

WPC Admin Columns 2.0.6 - 2.1.0 - Authenticated (Subscriber+) Privilege Escalation via User Meta Update

CONFIDENTIAL

The content of this document is intended solely for use by the natural or legal person to whom it is addressed. If you gain access to this document by mistake, you should be aware that any forwarding, copying or disclosure of its content to any other person is strictly prohibited, and you must inform the sender immediately.

Executive Summary

The WPC Admin Columns plugin for WordPress is vulnerable to privilege escalation in versions 2.0.6 to 2.1.0. This is due to the plugin not properly restricting user meta values that can be updated through the ajax_edit_save() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update their role to that of an administrator.

Analysis

An attacker with even a low-privilege Subscriber account can potentially gain full administrative access to a WordPress site. This could lead to complete site compromise, including: - Unauthorized changes to site settings - Installation of malicious plugins or themes - Creation of new admin accounts - Potential data theft or site defacement - Compromise of entire WordPress installation

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-3418

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/269.html

Versions affected

WPC Admin Columns plugin for WordPress affects versions

- 2.0.6
- 2.1.0

Solutions

1. Upgrade WPC Admin Columns plugin to a version beyond 2.1.0

2. Audit all user accounts, especially those with Subscriber or higher privileges

3. Implement additional access controls and monitoring

4. Use multi-factor authentication for admin accounts

5. Regularly review and restrict plugin permissions

6. Consider temporarily disabling the plugin if an update is not immediately available

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.