



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Actively Exploited Vulnerability in UpdraftPlus: WP Backup & Migration Plugin
Tracking #:432319124
Date:12-06-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the UpdraftPlus: WP Backup & Migration Plugin for WordPress could allow unauthenticated attackers to bypass authentication and execute administrative actions, potentially leading to remote code execution. The vulnerability is being actively targeted in the wild.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-10795**
- **Severity:** High | **CVSS:** 8.1
- The vulnerability stems from improper verification of cryptographic signatures and insufficient validation of remote communication messages within the UpdraftPlus_Remote_Communications_V2::wp_loaded function. An unauthenticated attacker can bypass signature verification, forge arbitrary RPC commands, and execute actions with the privileges of a connected administrator. This can lead to the upload and activation of malicious plugins, resulting in remote code execution on affected WordPress sites.
- Successful exploitation may allow malicious plugin installation and activation, ultimately resulting in remote code execution.

Affected Versions

- UpdraftPlus: WP Backup & Migration Plugin 1.26.4 and earlier.
- UpdraftPlus Premium – Versions prior to 2.26.5

Fixed Version:

- UpdraftPlus: WP Backup & Migration Plugin 1.26.5 or later.
- UpdraftPlus Premium 2.26.5 or later.

RECOMMENDATIONS:

- Apply the latest UpdraftPlus security update immediately.
- Review administrator accounts and installed plugins for suspicious activity.
- Enable web application firewall (WAF) protections and monitor for exploitation attempts.
- Maintain regular patch management practices for WordPress core, plugins, and themes.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://www.wordfence.com/blog/2026/06/critical-unauthenticated-authentication-bypass-vulnerability-patched-in-updraftplus-wordpress-plugin/>
- <https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/updraftplus/updraftplus-wp-backup-migration-plugin-1264-unauthenticated-authentication-bypass-via-updraftcentral-udrpc>