مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Remote Code Execution Vulnerability in GroupOffice

Tracking #:432318745

Date:07-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in GroupOffice, a popular open-source CRM and groupware suite. The flaw allows authenticated users, including low-privileged accounts, to achieve remote code execution (RCE) on affected servers.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE:** CVE-2026-34838
- **Severity:** Critical **CVSS Score:** 10.0 (Critical)
- The vulnerability exists in AbstractSettingsCollection.php and stems from unsafe handling of system settings. When a setting starts with the serialized: prefix, GroupOffice passes it to PHP's unserialize() function without class restrictions, allowing PHP Object Injection (POI).
- An attacker can inject a crafted object via a legacy HTTP endpoint. Using a POP chain with the Guzzle library, they can write a web shell to the filesystem, enabling full server control, including arbitrary command execution and data manipulation.

Fixed Versions

- GroupOffice 26.0.12, 25.0.90, 6.8.156 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by GroupOffice.

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://nvd.nist.gov/vuln/detail/CVE-2026-34838