مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerability in Roundcube Webmail

Tracking #:432317322

Date:29-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical post-authentication remote code execution (RCE) vulnerability has been discovered in Roundcube Webmail**.**

TECHNICAL DETAILS:

A critical post-authentication remote code execution (RCE) vulnerability has been discovered in Roundcube Webmail, impacting all versions from v1.1.0 to the current 1.6.10. Assigned **CVE-2025-48745**, this flaw enables any authenticated user to execute arbitrary code on the hosting server, potentially leading to complete system compromise. The bug has remained undetected for over a decade, placing over 53 million internet-facing servers at severe risk, including deployments integrated into popular hosting control panels like cPanel, Plesk, ISPConfig, and DirectAdmin.

This vulnerability shares characteristics with earlier Roundcube bugs that have been exploited by state-sponsored actors (e.g., APT28/GRU), underscoring its high exploitation potential. The vulnerability is trivially exploitable—1-click execution, with no need for WAF evasion. A patched version (v1.6.11) is expected shortly to be released by vendor.

RECOMMENDATIONS:

- Organizations using Roundcube must act immediately to mitigate exposure.
- Immediately limit Roundcube access to trusted IP addresses or behind a VPN until patching is complete.
- Audit server logs for unusual webmail behavior, especially from low-privilege accounts executing unexpected processes.

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: