مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in SmarterMail

Tracking #:432318192

Date:30-12-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in SmarterMail that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

A critical security vulnerability has been identified in SmarterMail, a widely used enterprise email and collaboration server. The flaw allows unauthenticated remote attackers to fully compromise affected mail servers. Exploitation requires no valid credentials and can result in complete system takeover.

Vulnerability Details

- **CVE-2025-52691**
- **Severity:** Critical
- **CVSS Score:** 10.0
- The vulnerability stems from improper handling of file upload functionality. Successful exploitation allows an attacker to upload arbitrary files to any location on the server. This can lead to remote code execution, enabling attackers to run malicious scripts and gain full control of the email server.

Affected Versions

- SmarterMail Build 9406 and earlier

Fixed Versions

- SmarterMail Build 9413 and later

RECOMMENDATIONS:

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

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-2025-52691