مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Actively Exploited Critical Vulnerability in SmarterTools SmarterMail

Tracking #:432318316

Date:27-01-2026

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 INTELLGIENCE 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 critical authentication bypass vulnerability has been discovered in SmarterTools SmarterMail, and it is actively being exploited in the wild.

TECHNICAL DETAILS:

A critical authentication bypass vulnerability has been identified in SmarterTools SmarterMail versions prior to Build 9511, tracked as CVE-2026-23760. The flaw allows unauthenticated attackers to reset system administrator passwords via an exposed password reset API endpoint without validation. Successful exploitation results in full administrative control of the SmarterMail application and can lead to operating system–level compromise of the underlying host.
This vulnerability is actively exploited in the wild and has been added to Known Exploited Vulnerabilities (KEV) Catalog, significantly increasing its risk profile. SmarterTools has released patched builds, and immediate remediation is strongly recommended.

Vulnerability Details

- CVE ID: CVE-2026-23760
- CWE: CWE-288 (Authentication Bypass Using an Alternate Path or Channel)
- CVSS v4.0 Score: 9.3 (Critical)
- Affected Versions: SmarterTools SmarterMail versions prior to build 9511 (all versions from initial release up to but not including 100.0.9511)
- Latest Version: Build 9518 (January 22, 2026) also include this and other critical security fixes
- Root Cause: The force-reset-password API endpoint accepts anonymous requests and includes a privileged path when the IsSysAdmin parameter is set to true. In this path, the code retrieves the administrator account by username, validates only the new password strength, and updates the password hash without checking the supplied OldPassword or any other authentication factor.

Impact:

- Immediate takeover of the system administrator account
- Full control over the SmarterMail instance (configuration, users, domains, mail flow)
- Ability to execute arbitrary OS commands as SYSTEM/root via the built-in "Volume Mount Command" feature in Settings → Volume Mounts, leading to host-level compromise
- Exploitation Status: Actively exploited in the wild.

RECOMMENDATIONS:

Prioritize Internet-Facing Instances:

- Identify and patch all SmarterMail servers exposed to the internet first, as the vulnerability requires only network access to the web interface.

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.smartertools.com/smartermail/release-notes/current
- https://www.cve.org/CVERecord?id=CVE-2026-23760