مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in SmarterTools SmarterMail

Tracking #:432318344

Date:03-02-2026

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 critical vulnerabilities in SmarterTools SmarterMail that could allow unauthorized system access, compromise of administrative accounts, or exposure of sensitive credentials.

TECHNICAL DETAILS:

Vulnerability Details:

1. **CVE-2026-24423 – Critical (CVSS 9.3)**
   - **Type:** Unauthenticated Remote Code Execution
   - **Description:** The ConnectToHub API method can be manipulated to point SmarterMail to a malicious HTTP server, causing the execution of OS commands on the host.
2. **CVE-2026-23760 – Critical (CVSS 9.3)**
   - **Type:** Authentication Bypass / Account Takeover
   - **Description:** The force-reset-password endpoint allows unauthenticated requests to reset system administrator passwords without verifying the existing password or reset token. Exploitation grants full administrative control, including the ability to execute OS commands on the host.
3. **CVE-2026-25067 – Medium (CVSS 6.9)**
   - **Type:** Path Coercion / NTLM Credential Exposure
   - **Description:** The background-of-the-day preview endpoint decodes attacker-controlled input into filesystem paths without validation. On Windows, this can trigger outbound SMB authentication to attacker-controlled hosts, enabling credential coercion, NTLM relay attacks, and unauthorized network authentication.

Impact:

Exploitation of these vulnerabilities could allow an unauthenticated attacker to fully compromise the SmarterMail instance, execute arbitrary commands on the underlying host, take over administrative accounts, and coerce network credentials for further lateral movement or privilege escalation.

Affected Products:

- SmarterMail versions prior to Build 9511
- SmarterMail versions prior to Build 9518

Fixed Versions:

- SmarterMail Build 9511
- SmarterMail Build 9518

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by SmarterTools.

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-2026-24423
- https://nvd.nist.gov/vuln/detail/CVE-2026-23760
- https://nvd.nist.gov/vuln/detail/CVE-2026-25067