

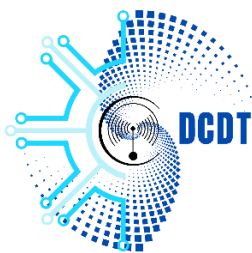
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOUVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

10 September 2026

Advisory 294: SmarterMail Critical Authentication Bypass, Unrestricted File Upload, and Unauthenticated Remote Code Execution - Active Ransomware Exploitation (CVE-2025-52691, CVE-2026-23760, and CVE-2026-24423).

Release Date: 9th September 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This advisory is relevant to system and network administrators who operate SmarterTools SmarterMail (on-premises) as an email and collaboration server, including hosting providers, ISPs, and organizations running SmarterMail for internal or externally-facing mail services. This alert is intended primarily for a technical audience.

What is it?

CVE-2025-52691, CVE-2026-23760, and CVE-2026-24423 are three critical vulnerabilities in SmarterTools SmarterMail, a commercial on-premises email and collaboration server, disclosed in a cluster between late December 2025 and late January 2026 and combined into this single advisory because they were disclosed in the same wave of vendor patches, share the same affected on-premises deployment scope, and are resolved together in build 9511.

CVE-2025-52691 is an unrestricted upload of a dangerous file type (CWE-434), CVE-2026-23760 is an authentication bypass in SmarterMail's password-reset API (CWE-288) that lets an unauthenticated attacker reset a system administrator's password with a single crafted HTTP request, and CVE-2026-24423 is a missing-authentication flaw (CWE-306) in SmarterMail's ConnectToHub API that gives an unauthenticated remote attacker direct code execution.

What are the systems affected?

The following version(s) are affected:

- SmarterMail (on-premises) prior to build 9511 - (Affected)

SmarterMail (on-premises) build 9511 and later - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Identify an internet-facing SmarterMail server and reach it through one of two unauthenticated entry points**
 - An attacker sends a single crafted HTTP request either to the password-reset API endpoint (CVE-2026-23760) to reset a system administrator's password without any prior credentials, or to the ConnectToHub API (CVE-2026-24423), which is missing an authentication check entirely and grants direct code execution. A third path exists via CVE-2025-52691, uploading a file of a dangerous type through an unrestricted upload endpoint to plant a webshell.
2. **Establish persistence and stage ransomware**
 - Once administrator access or code execution is achieved, the attacker abuses SmarterMail's built-in "Volume Mount" feature to reach the underlying filesystem and gain full system control, installs the Velociraptor digital forensics and incident response tool to maintain covert access, and stages a ransomware payload for deployment. The pattern observed in confirmed Warlock/Storm-2603 intrusions.

Attack vectors:

- A network-based attack requiring no authentication and no user interaction. Any of the three vulnerabilities can be reached directly by an attacker with network access to the SmarterMail server's web-facing API.
- All three CVEs are confirmed under active exploitation.

Mitigation process

CERTVU recommends the following:

1. Apply the SmarterMail update immediately
 - Update SmarterMail to build 9511 or later without delay. Given confirmed active exploitation and confirmed local exposure, this should be treated as an emergency change rather than scheduled maintenance.

2. Audit for signs of prior compromise before and after patching
3. Restrict administrative and API access to the SmarterMail server
4. Rotate credentials and review for persistence mechanisms

Report any suspected compromise arising from these vulnerabilities to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2025-52691>
2. <https://www.cve.org/CVERecord?id=CVE-2026-23760>
3. <https://www.cve.org/CVERecord?id=CVE-2026-24423>
4. <https://www.cisa.gov/news-events/alerts/2026/01/26/cisa-adds-five-known-exploited-vulnerabilities-catalog>
5. <https://www.helpnetsecurity.com/2026/02/06/ransomware-smartermail-cve-2026-24423/>