Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Unpatched SmarterMail Servers Become Launchpads for Ransomware Operations

Date of Publication	Last Update Date	Admiralty Code	TA Number
February 09, 2026	February 11, 2026	A1	TA2026040

Summary

First Seen: 2026
Affected Products: SmarterTools SmarterMail
Actor: Storm-2603
Malware: Warlock Ransomware
Impact: Attackers are actively exploiting critical SmarterMail vulnerabilities CVE-2026-23760 and CVE-2026-24423 to take over administrator accounts and remotely execute commands on exposed servers, effectively turning email systems into entry points for wider network compromise. Campaigns linked to the Storm-2603 group show how these flaws can quickly escalate into ransomware staging operations, with attackers disguising malicious actions as normal system activity and even abusing legitimate security tools to remain undetected. This further highlights systemic risks in unpatched deployments, and with multiple actors already scanning for vulnerable systems, organizations running outdated SmarterMail versions face immediate takeover risks unless they update without delay.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-24423	SmarterTools SmarterMail Missing Authentication for Critical Function Vulnerability	SmarterTools SmarterMail	✗	✓	✓
CVE-2026-23760	SmarterTools SmarterMail Authentication Bypass Using an Alternate Path or Channel Vulnerability	SmarterTools SmarterMail	✗	✓	✓

Vulnerability Details

#1

Two serious vulnerabilities have been identified in SmarterTools SmarterMail, both affecting versions released before Build 9511. The first, CVE-2026-23760, stems from a weakness in the platform's password reset mechanism, which fails to properly verify who is requesting a reset. As a result, an unauthenticated attacker can simply provide an administrator's username and assign a new password, effectively taking over accounts without needing any prior access. SmarterTools resolved this issue in Build 9511, closing the door on this direct authentication bypass.

#2

A second and even more dangerous flaw, tracked as CVE-2026-24423, allows attackers to execute commands remotely on vulnerable servers without authentication. The issue lies in the ConnectToHub API endpoint, which does not properly check whether requests come from an authorized administrator. Attackers can trick the server into connecting to infrastructure they control, then feed it malicious configuration data that ultimately triggers command execution on the underlying system. Because this process requires no user interaction and can be automated, exposed SmarterMail servers quickly become attractive targets for widespread attacks.

#3

These weaknesses are already being exploited in the wild. CVE-2026-23760 has been linked to activity attributed to the China-based group Storm-2603, which used the flaw to gain administrative control before executing commands through SmarterMail features. Security researchers have also observed exploitation attempts from infrastructure unrelated to Storm-2603, suggesting that multiple groups or automated campaigns are racing to abuse these flaws.

#4

Investigations show that exploitation of these flaws is closely tied to attempts to deploy Warlock ransomware. Attackers first used CVE-2026-23760 to gain administrative access, then leveraged SmarterMail's Volume Mount feature to pivot from application control to system-level command execution. From there, they abused the Windows Installer utility to download a malicious MSI package hosted on Supabase, disguising the activity as routine system operations. The move from previously used hosting platforms to new infrastructure appears to be a deliberate tactic to evade existing detection and blocking mechanisms.

#5 The downloaded MSI package installs Velociraptor, a legitimate incident response tool, which attackers repurpose as a stealthy command-and-control channel. Because the tool is commonly used by security teams, its presence is less likely to raise suspicion, allowing attackers to maintain access while preparing for ransomware deployment. Although ransomware was not ultimately executed in the observed incidents, the techniques used closely match known Warlock ransomware operations, indicating the attack was likely interrupted during its staging phase. With multiple SmarterMail vulnerabilities already under active exploitation, organizations are strongly advised to upgrade to Build 9511 or later immediately to prevent compromise.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-24423	SmarterTools SmarterMail (Before Build 9511)	cpe:2.3:a:smartertools:smartermail:*:*:*:*:*:*:*:*	CWE-306
CVE-2026-23760	SmarterTools SmarterMail (Before Build 9511)	cpe:2.3:a:smartertools:smartermail:*:*:*:*:*:*:*:*	CWE-288

Recommendations

Upgrade SmarterMail Immediately: Upgrade all SmarterTools SmarterMail instances to Build 9511 or later without delay. This build addresses both CVE-2026-23760 and CVE-2026-24423, closing the authentication bypass and remote code execution vulnerability gaps. Given the observed active exploitation by ransomware operators, this should be treated as an emergency priority for any organization running internet-facing SmarterMail instances.

Audit Server Logs for Suspicious Activity: Security teams should immediately review SmarterMail server logs for any unauthorized interactions with the /api/v1/settings/sysadmin/connect-to-hub endpoint. Any unexpected POST requests to this API path, particularly those originating from external IP addresses or containing unusual hubAddress parameters, should be treated as potential indicators of compromise and investigated thoroughly.

Restrict Network Access to Administrative APIs: As an interim mitigation measure, organizations should implement network-level access controls to restrict access to SmarterMail administrative API endpoints. Deploying web application firewalls (WAF) or reverse proxy rules to block unauthenticated external requests to the /api/v1/settings/sysadmin/ path can reduce the attack surface while patching is underway.

Implement Network Segmentation: Email servers should be isolated within a dedicated network segment with strict ingress and egress controls. This limits the blast radius if a SmarterMail instance is compromised, preventing attackers from easily pivoting to other critical infrastructure components within the organization's network.

Vulnerability Management: Organizations should maintain a rigorous vulnerability management program that includes regular scanning and assessment of all internet-facing applications and services. Maintaining a current inventory of software versions and security patches is essential, and the security practices of third-party vendors, particularly for critical services such as email platforms, should be evaluated and monitored on an ongoing basis.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Privilege Escalation	T1078: Valid Accounts	
	T1068: Exploitation for Privilege Escalation	
Defense Evasion	T1218: System Binary Proxy Execution	T1218.007: Msiexec
	T1036: Masquerading	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols

Tactic	Technique	Sub-technique
Impact	T1486: Data Encrypted for Impact	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	auth[.]qgtxtebl[.]workers[.]dev, vdfccjpnedujhrzscjtq[.]supabase[.]co, 2-api[.]mooo[.]com
IPv4	162[.]252[.]198[.]197, 199[.]217[.]99[.]93, 157[.]245[.]156[.]118, 45[.]127[.]35[.]186, 178[.]128[.]103[.]218

Patch Link

https://www.smartertools.com/smartermail/release-notes/current

References

https://www.vulncheck.com/advisories/smartertools-smartermail-unauthenticated-rce-via-connecttohub-api

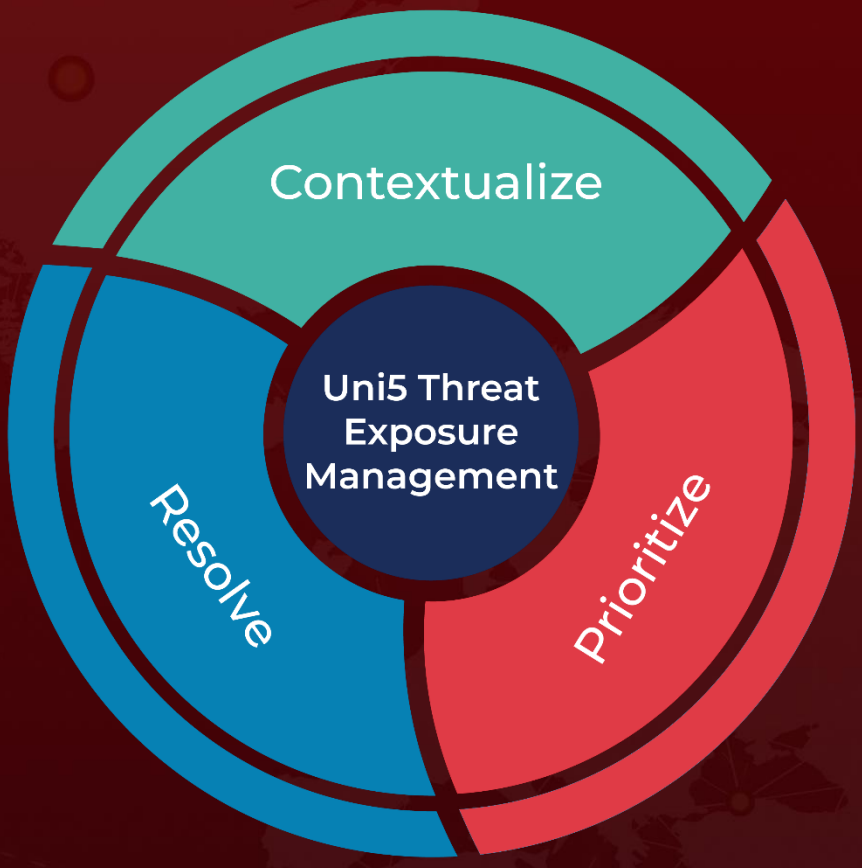
https://www.sentinelone.com/vulnerability-database/cve-2026-24423/

https://reliaquest.com/blog/threat-spotlight-storm-2603-exploits-CVE-2026-23760-to-stage-warlock-ransomware/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 09, 2026 • 7:30 AM

More at www.hivepro.com