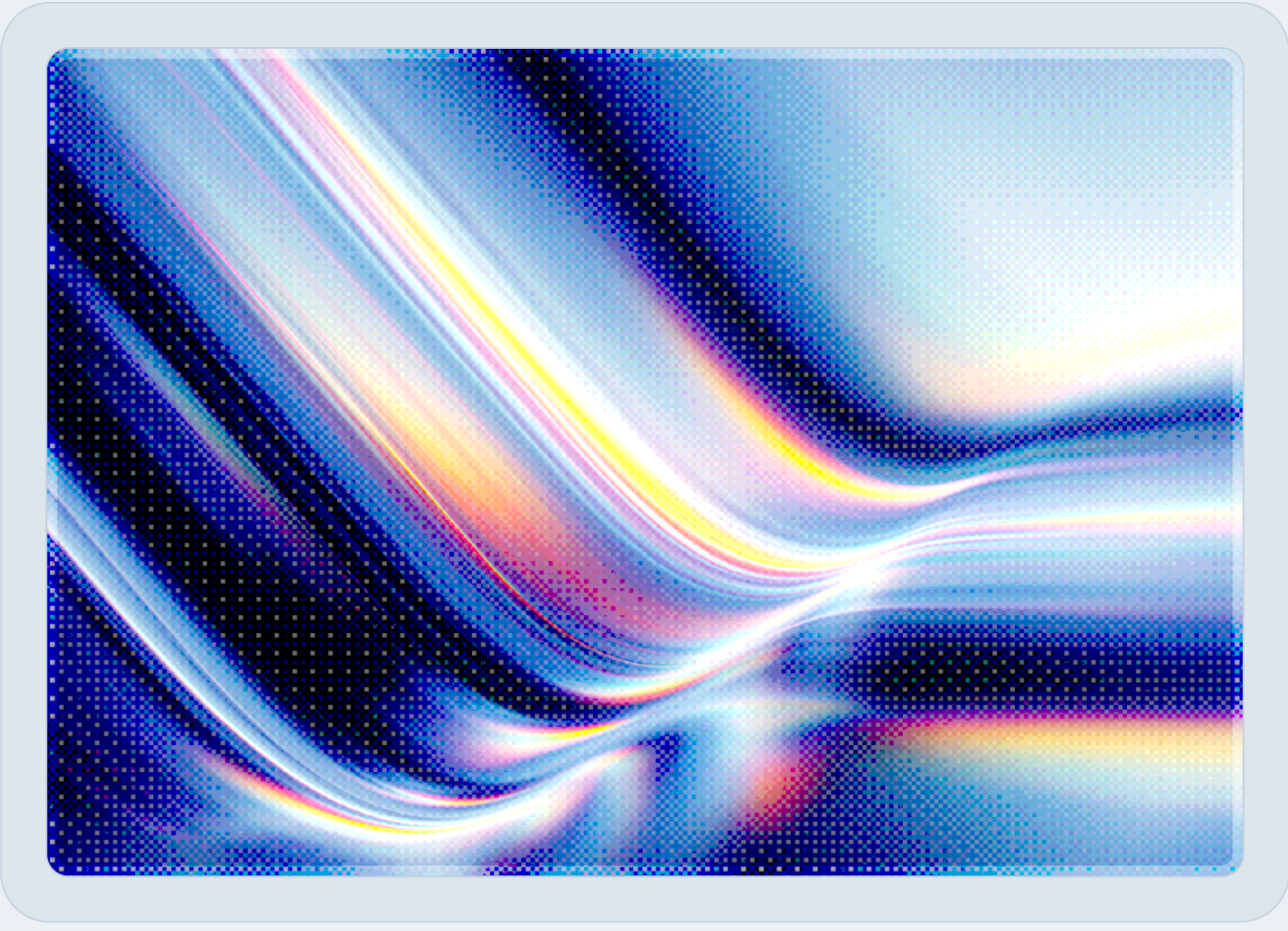
CSAI Foundation | Cloud Security Alliance

Trusted Update Channels as Credential Stealer Delivery Vectors

CVE-2026-35616 and the Weaponization of FortiClient EMS: How Attackers Turn Enterprise Security Management Infrastructure Against the Endpoints It Protects

2026-05-30

AI-assisted Rapid Research



CSAI

cloud security alliance®

Key Takeaways

- CVE-2026-35616 (CVSS 9.1) is a pre-authentication API access bypass in FortiClient EMS 7.4.5 and 7.4.6 that allows unauthenticated remote code execution; it was added to the CISA Known Exploited Vulnerabilities catalog on April 6, 2026, and active exploitation campaigns continue as of late May 2026.
- Threat actors exploiting this vulnerability are not merely breaching the EMS server — they are using it as a force multiplier, weaponizing its legitimate VPN on_connect script-push capability to simultaneously deliver credential-stealing malware (EKZ Infostealer, disguised as a Fortinet patch) to every managed endpoint in the organization.
- This campaign is an instance of a documented and accelerating attack pattern: compromise the trusted management plane, then use that plane's own privileged delivery mechanism to push payloads that endpoint defenses will not scrutinize.
- FortiClient EMS is the second of the two major attack patterns in 2026's first half — alongside RMM-based lateral movement — that exploit the architectural assumption that enterprise management tooling occupies a trusted, implicitly authorized position in the network.
- Organizations running FortiClient EMS 7.4.5 or 7.4.6 should treat patching to 7.4.7 (or applying the out-of-band hotfix) as an emergency, and should immediately audit EMS configuration for unauthorized changes to Remote Access Profiles and on_connect script directives.

Background

FortiClient Endpoint Management Server is Fortinet's centralized platform for deploying, configuring, and monitoring the FortiClient security agent across enterprise endpoints. It is designed to operate at scale — a single EMS instance can manage more than 50,000 endpoints — and it occupies a privileged architectural position in Fortinet Security Fabric deployments [1]. EMS functions as a private certificate authority, a policy enforcement point, and a software distribution server simultaneously. It pushes configuration profiles, VPN tunnel parameters, antivirus signatures, and software updates to every registered endpoint over a persistent Telemetry channel (TCP 8013 by default). The trust relationship is largely unidirectional by design: once an endpoint has registered and validated EMS's SSL certificate, it

accepts configuration changes and software deliveries from the server without further per-command authentication [2]. This architecture is appropriate and efficient for legitimate operations, but it means that whoever controls EMS effectively controls every endpoint on the platform.

The historical record of FortiClient EMS is a useful lens for understanding the current threat environment. CVE-2023-48788, a critical SQL injection in EMS's Database Access Service component, was disclosed in March 2024 with a CVSS score of 9.8. Proof-of-concept exploit code appeared within nine days of disclosure, and Fortinet confirmed active exploitation the same day. Medusa ransomware operators subsequently used that vulnerability for initial access in attacks documented through 2024 [3] [4]. CVE-2026-21643, a separate pre-authentication SQL injection in EMS 7.4.4, was added to the CISA KEV catalog in April 2026 alongside CVE-2026-35616 [5]. CISA has now added 24 Fortinet product vulnerabilities to its KEV catalog, with the majority involved in ransomware campaigns [6]. The pattern is not accidental: EMS is a high-value target precisely because its compromise delivers not just access to one server but programmatic authority over every endpoint in the organization.

CVE-2026-35616 was first detected as a zero-day by watchTowr honeypot infrastructure on March 31, 2026 [7][25]. Fortinet published its advisory (FG-IR-26-099) and released an out-of-band hotfix on April 4, 2026, crediting researchers Simo Kohonen of Defused and Nguyen Duc Anh for responsible disclosure [7]. CISA added the vulnerability to the KEV catalog on April 6, 2026, giving federal civilian branch agencies a seventy-two-hour remediation deadline [8][30]. Arctic Wolf's threat intelligence team published a detailed campaign analysis on May 27, 2026 [9][26][27], documenting active exploitation of the vulnerability continuing more than seven weeks after patch availability, with a specific focus on the credential stealer payload being delivered through EMS's own update mechanism. Approximately 2,000 or more FortiClient EMS instances remain publicly reachable on the internet [10], and the campaign was still active at the time of the Arctic Wolf report.

Security Analysis

The Attack Pattern

The exploitation of CVE-2026-35616 is technically a network intrusion, but functionally it is a supply chain attack [29] delivered from inside the target organization's own management infrastructure. The distinction matters for defenders. A conventional malware delivery campaign requires the attacker to breach the perimeter, establish persistence, evade endpoint detection, and then move laterally to reach credentials. In the EKZ Infostealer campaign documented by Arctic Wolf [9], the attacker bypassed all of those steps by reaching the EMS server first and then using EMS's own privileged delivery channel to

simultaneously push credential-harvesting payloads to every endpoint in the organization. The endpoint agents received the payload from their trusted management server, executed it with system-level privileges, and did not flag it as anomalous — because the delivery was, from the agent's perspective, indistinguishable from a legitimate update.

This attack pattern has appeared repeatedly in the past decade, each time through a different management platform but following the same structural logic. REvil's July 2021 compromise of Kaseya VSA delivered ransomware to approximately 1,500 downstream businesses by weaponizing VSA's auto-update pipeline; the payload was disguised as a legitimate VSA maintenance update to prevent detection [11]. APT29's insertion of the SUNBURST backdoor into SolarWinds Orion builds reached approximately 18,000 organizations through the legitimate update distribution mechanism — a figure SolarWinds disclosed in its own SEC filings during the subsequent investigation [12]. In May 2026, Microsoft Incident Response documented a campaign in which attackers abused the HPE Operations Agent — a legitimate enterprise monitoring tool — to push malicious scripts to managed servers for more than 100 days without triggering behavioral detection, because the activity was indistinguishable from routine administrative operations [13]. The FortiClient EMS campaign fits this pattern precisely: a trusted management agent with privileged software execution authority becomes the malware delivery vector.

What distinguishes the 2026 wave of these attacks from earlier incidents is the consistent targeting of credential material rather than immediate encryption or destruction. EKZ Infostealer implements Chromium v20 AES-256 decryption to bypass Chrome's encrypted password storage, extracts session cookies capable of replaying authenticated sessions without re-entering credentials (and thus bypassing multi-factor authentication), and harvests saved passwords and autofill data from Chrome, Edge, Chromium, and Firefox [9]. The extracted credentials and cookies are staged locally in C:\ProgramData\log.txt before exfiltration to attacker-controlled infrastructure. Session cookie theft is particularly significant: it enables attackers to access cloud services, SaaS applications, and identity provider sessions that were protected by MFA at login time but become unprotected once the authenticated session token is in attacker hands.

Technical Mechanics

CVE-2026-35616 is classified as an Improper Access Control flaw (CWE-284) in the FortiClient EMS API. The vulnerability allows an unauthenticated remote attacker to send specially crafted HTTP requests that the API processes as privileged administrative actions, bypassing authentication and authorization checks entirely. No credentials, no user interaction, and no prior foothold in the environment are required, which the CVSS vector (AV:N/AC:L/PR:N/UI:N) reflects [7]. Affected versions are FortiClient EMS 7.4.5 and 7.4.6 exclusively; the 7.2.x series and below are not affected. The out-of-band hotfix for 7.4.5 and 7.4.6 requires no downtime, and the permanent fix is included in 7.4.7 [7].

Once an attacker achieves unauthenticated RCE on the EMS server, the observed attack chain proceeds through three stages. First, the attacker modifies the Remote Access Profile and endpoint policies within EMS, gaining control over what configuration and scripts are distributed to managed endpoints. Second, the attacker weaponizes the VPN on_connect directive, a legitimate EMS feature that executes scripts when a managed endpoint establishes a VPN tunnel. Malicious PowerShell scripts are inserted into this directive and pushed to all registered endpoints. Third, endpoints download and execute a file named FortiEndpoint_Patch.exe from attacker-controlled infrastructure at 83.138.53.110, disguised as a Fortinet endpoint patch; this file is the EKZ Infostealer, compiled as a PE32+ x86-64 console executable with a SHA-256 hash of 0da123adf9251957a4b850a3f6bd6a753dd4892be176a84a18450e899534cc5e [9]. The entire payload delivery chain executes silently in the background, removes local execution artifacts, and leaves no obvious user-facing indication that anything has occurred.

Fortinet has recommended restricting network access to the EMS management port (TCP 8013) as a compensating control for organizations unable to apply the patch immediately [7]. This is the correct architectural principle: an endpoint management server that must be reachable from the public internet to function has a structurally elevated attack surface that compensating network controls can partially mitigate.

Threat Actor Implications

The EKZ Infostealer campaign is not an isolated incident but a representative example of a broader evolution in how attackers approach enterprise credential theft at scale. MITRE ATT&CK's T1072 (Software Deployment Tools) [28] catalogs this pattern with examples spanning Medusa ransomware's abuse of BigFix and PDQ Deploy [14], APT32's historical compromise of McAfee ePolicy Orchestrator to distribute malware as a software deployment task [15], and VOID MANTICORE's March 2026 use of stolen Microsoft Intune administrative credentials to issue bulk factory-reset commands that idled more than 56,000 Stryker Corporation employees across 79 countries [16]. In the Stryker incident, no vulnerability was exploited — the legitimate Intune API was abused with valid administrative credentials, producing no EDR signal and no malware signature to detect.

Huntress reported a 277 percent year-over-year increase in RMM tool abuse between 2024 and 2025 [17]. Arctic Wolf's 2025 Threat Report found that 59.4 percent of ransomware incident response engagements began with external remote access abuse, including RMM exploitation, and that malicious use of 32 different RMM tools was observed across cases [18]. Microsoft Defender Experts documented coordinated zero-day exploitation across ConnectWise ScreenConnect (CVE-2024-1709, CVSS 10.0), BeyondTrust Remote Support (CVE-2024-12356, CVSS 9.8), and SimpleHelp during the same period

[19]. The structural driver is straightforward: a single compromised management platform provides simultaneous reach to every endpoint it manages, making it a dramatically more efficient target than attacking individual endpoints one at a time.

The credential-harvesting focus of the current campaign wave also reflects a strategic maturation. Stolen session cookies and browser-stored credentials provide access to cloud infrastructure, SaaS applications, and identity providers that are architecturally separate from the on-premises environment where the initial breach occurred. An organization that segments its on-premises network effectively and deploys EDR across all endpoints may still experience cloud environment compromise if session cookies from those endpoints are exfiltrated before the breach is detected.

Recommendations

Immediate Actions

Organizations running FortiClient EMS should take the following steps immediately, treating each as an emergency action rather than a scheduled maintenance task.

The first priority is applying the patch: upgrade to FortiClient EMS 7.4.7 or install the out-of-band hotfix for 7.4.5 and 7.4.6 without delay. Fortinet confirmed the hotfix requires no downtime. FortiClient Cloud and FortiSASE customers were patched server-side and require no customer action [7].

Concurrent with patching, audit EMS configuration for unauthorized changes, specifically examining Remote Access Profile settings and any VPN on_connect or on_disconnect script directives for entries that were not administratively created. Any scripts referencing external IP addresses or download locations that were not explicitly configured by your team should be treated as indicators of compromise.

For threat hunting purposes, block or alert on network connections from managed endpoints to 83.138.53.110, and search endpoint logs for execution of FortiEndpoint_Patch.exe. Examine C:\ProgramData\log.txt on endpoints for the presence of harvested credential data staged by EKZ Infostealer. The file hashes documented by Arctic Wolf (SHA-256: 0da123adf9251957a4b850a3f6bd6a753dd4892be176a84a18450e899534cc5e; MD5: 338662fd0c4d750a0ba203a32b59f081) should be added to your threat intelligence and detection tooling [9].

If compromise of EMS is confirmed or suspected, invalidate all active browser sessions and force re-authentication across your SaaS and cloud environment. Stolen session cookies can persist after password resets if the underlying session token has not been revoked.

Short-Term Mitigations

Restrict network access to TCP 8013 (the EMS Telemetry channel) to only the IP ranges that require it. An EMS server that is reachable from the public internet without network access controls is fully exposed to unauthenticated exploitation of any API vulnerability. This is Fortinet's own recommended compensating control and applies to EMS deployments regardless of patch status [7].

Implement monitoring on the EMS server for configuration changes to Remote Access Profiles and script directives, specifically alerting on changes made outside of approved change management windows or from unexpected source IPs. The Arctic Wolf campaign succeeded in part because the configuration changes made on the EMS server were not flagged; visibility into administrative actions on management infrastructure is a prerequisite for detecting this class of attack.

Review all enterprise RMM, MDM, and endpoint management platforms — not only FortiClient EMS — for similar exposure. The CISA/NSA joint advisory on RMM abuse [20] and Microsoft's documentation of the broader management platform threat landscape [19] make clear that this is a systemic attack surface, not a Fortinet-specific problem. ConnectWise ScreenConnect, BeyondTrust Remote Support, and SimpleHelp have all faced critical vulnerabilities with active exploitation in the 2024–2026 window.

Strategic Considerations

The EKZ Infostealer campaign illustrates why Zero Trust principles must extend to management infrastructure, not just to user endpoints. The foundational Zero Trust assumption — that no entity should be implicitly trusted based on its network position — applies equally to the management server that distributes security policy. Continuous verification of administrative actions, separation of duties for EMS configuration changes, and network segmentation of the management plane from the production endpoint network are structural controls that would limit the blast radius of a compromised EMS server even when a patch has not yet been applied.

Organizations should examine whether their browser credential exposure extends beyond the workstations directly managed by EMS. If credentials for cloud infrastructure, identity providers, or SaaS applications are stored in browsers on managed endpoints, a single EMS compromise creates a credential exposure event across the entire cloud estate. Privileged access workstations for cloud and identity administration should store credentials in dedicated credential managers rather than browser stores, and should not be in scope for bulk EMS-driven software delivery.

The software supply chain security controls outlined in CSA's Cloud Controls Matrix supply chain management domain provide a framework for extending update integrity verification requirements to vendor-managed update channels. While CCM controls were designed primarily for cloud service providers, the underlying principle — that every software artifact delivered to a managed system should have a verifiable, tamper-evident chain of custody — applies directly to the EMS update delivery problem. Organizations should evaluate whether their endpoint management platforms offer signed-update verification that endpoints can validate independently of the management server's integrity.

CSA Resource Alignment

The FortiClient EMS attack pattern maps directly to CSA's Cloud Controls Matrix Supply Chain Management (STA) domain, which was significantly expanded in CCM v4.1 to address software supply chain and trusted vendor delivery risks [21]. The specific controls addressing supplier assurance, software integrity verification, and update authorization are relevant both to how organizations assess the security posture of tools like EMS before deployment and to how they detect deviations in those tools' behavior at runtime. The broader AICM framework, which extends CCM controls to AI-enabled and autonomously operating systems, is also applicable here: as endpoint management platforms incorporate AI-driven policy automation and autonomous remediation capabilities, the control plane abuse documented in this campaign becomes a higher-stakes attack surface.

CSA's Zero Trust work is equally germane. The Zero Trust Guidance for Achieving Operational Resilience [22] and the Zero Trust Advancement Center's published frameworks address the architectural principle that management plane access must be subject to the same continuous verification requirements as user access — an assumption the EMS campaign's architecture directly violated. The principle that trust is never implicit, always verified, and scoped to the minimum necessary access should govern how EMS administrative credentials are issued, how configuration changes are authorized, and how the management channel's network exposure is bounded.

CSA's software supply chain security publications, including the 2026 CSA blog post "Software Supply Chain Security Needs an Upgrade" [23] and the Top Threats to Cloud Computing 2025 artifact [24] — which addresses supply chain risks among the critical categories of concern in cloud security — provide organizational context for treating trusted update delivery mechanisms as a security-critical attack surface rather than an administrative convenience. The documented threat actor ecosystem described in this research note, from APT29's SolarWinds compromise through REvil's Kaseya VSA attack to the current EKZ Infostealer campaign, represents more than five years of adversarial refinement of a single

structural attack pattern. Defenders who have not yet applied the architectural controls — management plane network isolation, update integrity verification, and privileged access governance — that would contain this pattern are operating with a known and actively exploited blind spot.

References

[1] Fortinet. "FortiClient EMS Administration Guide, 7.4.7." Fortinet Documentation, 2026.

[2] Fortinet. "Establish Device Identity and Trust Context with FortiClient EMS." FortiOS 8.0 Administration Guide, 2026.

[3] Darktrace. "FortiClient EMS Exploited: Inside the Attack Chain and Post-Exploitation Tactics." Darktrace Blog, 2024.

[4] Horizon3.ai. "CVE-2023-48788: Fortinet FortiClientEMS SQL Injection Deep Dive." Horizon3.ai Attack Research, March 2024.

[5] Fortinet PSIRT. "FG-IR-25-1142: CVE-2026-21643." Fortinet PSIRT Advisory, 2026.

[6] CISA. "Known Exploited Vulnerabilities Catalog." Cybersecurity and Infrastructure Security Agency, 2026.

[7] Fortinet PSIRT. "FG-IR-26-099: CVE-2026-35616." Fortinet PSIRT Advisory, April 4, 2026.

[8] Canadian Centre for Cyber Security. "AL26-007: Vulnerability Impacting Fortinet FortiClientEMS (CVE-2026-35616)." CCCS Alert, April 2026.

[9] Arctic Wolf. "FortiClient EMS Exploited via CVE-2026-35616 to Deliver EKZ Infostealer Disguised as a Fortinet Patch." Arctic Wolf Blog, May 27, 2026.

[10] CyberPress. "Over 2,000 FortiClient EMS Servers Exposed as RCE Attacks Surge." CyberPress, 2026.

[11] Varonis. "REvil MSP Supply Chain Attack." Varonis Blog, 2021.

[12] Palo Alto Unit42. "SolarStorm Supply Chain Attack Timeline." Unit 42 Threat Intelligence, 2020.

[13] Microsoft Security. "Undermining the Trust Boundary: Investigating a Stealthy Intrusion Through Third-Party Compromise." Microsoft Security Blog, May 12, 2026.

[14] CISA. "#StopRansomware: Medusa Ransomware (AA25-071A)." CISA Cybersecurity Advisory, March 2025.

[15] MITRE ATT&CK. "APT32 (G0050)." MITRE ATT&CK, 2024.

[16] BlackVeil Security. "Stryker Iran Wiper Attack 2026-03-12." BlackVeil Security Blog, March 2026.

[17] Huntress. "RMM Abuse: When IT Convenience Bites Back." Huntress Blog, 2025.

[18] Arctic Wolf. "Understanding the Risks of Remote Monitoring and Management Tools." Arctic Wolf 2025 Threat Report, 2025.

[19] Microsoft Security Experts. "Keys to the Kingdom: RMM Exploits Enabling Human-Operated Intrusions in 2024–25." Microsoft Community Hub, 2025.

[20] CISA / NSA. "Protecting Against Malicious Use of Remote Monitoring and Management Software." CISA/NSA Joint Cybersecurity Advisory, January 2023.

[21] Cloud Security Alliance. "The CSA Cloud Controls Matrix v4.1: Strengthening the Future of Cloud Security." CSA Blog, December 2025.

[22] Cloud Security Alliance. "Zero Trust Guidance for Achieving Operational Resilience." CSA Artifacts, 2025.

[23] Cloud Security Alliance. "Software Supply Chain Security Needs an Upgrade." CSA Blog, April 2026.

[24] Cloud Security Alliance. "Top Threats to Cloud Computing 2025." CSA Artifacts, 2025.

[25] watchTowr. "Fortinet FortiClient EMS Zero-Day CVE-2026-35616: Active Exploitation Underway." watchTowr Research, April 2026.

[26] BleepingComputer. "Hackers Exploit FortiClient EMS Flaw to Push Infostealer Malware." BleepingComputer, May 2026.

[27] The Hacker News. "Threat Actors Exploit Critical FortiClient EMS Flaw to Deploy Credential Stealer." The Hacker News, May 2026.

[28] MITRE ATT&CK. "T1072: Software Deployment Tools." MITRE ATT&CK, 2024.

[29] MITRE ATT&CK. "T1195.002: Compromise Software Supply Chain." MITRE ATT&CK, 2024.

[30] NVD. "CVE-2026-35616." National Vulnerability Database, April 2026.

