CSAI Foundation

Cloud Security Alliance AI Safety Initiative

FortiClient EMS Zero-Day: Pre-Auth API Bypass Exploited

CVE-2026-35616, Active Zero-Day Exploitation, and the FortiClient EMS Vulnerability Chain

Unofficial AI-assisted Research

2026-04-05

Key Takeaways

- CVE-2026-35616 is a critical (CVSS 9.1 per Fortinet advisory) pre-authentication API bypass in Fortinet FortiClient EMS 7.4.5 and 7.4.6, disclosed April 4, 2026, with confirmed active exploitation beginning March 31, 2026 — a zero-day window that opened over the Easter holiday weekend [1].
- The vulnerability allows an unauthenticated remote attacker to bypass all API authentication and authorization, enabling arbitrary command execution with no credentials and no user interaction required [1, 2].
- Organizations that patched CVE-2026-21643 (a critical SQL injection in FortiClient EMS 7.4.4, exploited from March 26) by upgrading to version 7.4.5 immediately acquired CVE-2026-35616 — a back-to-back critical zero-day chain across consecutive releases [3, 15].
- Emergency hotfixes (7.4.5.2111 and 7.4.6.2170) are available now; FortiClient EMS 7.4.7, the permanent patch release, was announced as an upcoming release at time of advisory publication [1].
- Historical exploitation of CVE-2023-48788 — a pre-authentication SQL injection in FortiClient EMS that similarly enabled unauthenticated remote code execution — suggests that successful compromise may lead to ransomware deployment, credential theft, and lateral movement using commodity remote management tools [6, 7].
- Approximately 2,000 to 2,400 FortiClient EMS instances are directly accessible from the internet, the majority concentrated in the United States and Europe [3, 4, 15].

Background

Fortinet FortiClient EMS (Endpoint Management Server) is the centralized management and policy enforcement component of Fortinet's endpoint security ecosystem. Deployed on-premises, it serves as the administrative backbone for FortiClient installations across an organization's endpoint fleet — enforcing security posture requirements, issuing VPN configurations, and acting as the control plane for Fortinet's Zero Trust Network Access (ZTNA) telemetry fabric [1]. Because FortiClient EMS is typically

network-accessible to managed endpoints and sometimes exposed to the broader internet, it represents a high-value target: compromising it can grant an attacker administrative control over endpoint policy, the ability to manipulate compliance data, and a persistent foothold deep within the network.

Fortinet has an established history of critical vulnerabilities in its enterprise products, and FortiClient EMS has been a recurring target. CVE-2023-48788, a SQL injection vulnerability disclosed in March 2024 carrying a CVSS score of 9.8 [16], attracted widespread exploitation activity following disclosure, documented in post-compromise analysis by Darktrace, Kaspersky, and Horizon3.ai [6, 7, 8]. Post-exploitation telemetry from that campaign revealed a consistent attack playbook: initial access through the exposed application port, deployment of legitimate remote monitoring and management (RMM) tools such as ScreenConnect, AnyDesk, and Atera to establish persistence, followed by credential harvesting using Mimikatz and WebBrowserPassView, lateral movement through PsExec and WMI, and in at least one documented case, the deployment of Medusa ransomware approximately three weeks after initial access [6, 7, 8]. The attacker infrastructure observed in those campaigns included IP addresses linked to Russian autonomous system numbers and command-and-control domains designed to blend with legitimate cloud services [7].

That history establishes a realistic threat model for current incident response: organizations should anticipate an attacker playbook that extends well beyond initial access. CVE-2026-35616, published on April 4, 2026 under Fortinet advisory FG-IR-26-099, represents a new critical-severity pre-authentication vulnerability in the same product, and exploitation was already underway when the patch was issued [1].

Security Analysis

CVE-2026-35616: Technical Profile

CVE-2026-35616 is classified as an Improper Access Control flaw (CWE-284) affecting the API layer of FortiClient EMS. The vulnerability allows a specially crafted network request to bypass all authentication and authorization checks enforced at the API boundary, meaning an attacker with nothing more than network access to the EMS server can issue API calls as if they were an authenticated administrator [1, 2]. The CVSS 3.1 base score is 9.1 per the official Fortinet advisory [1]; all major sources consulted confirm the Critical severity rating. The CVSS attack vector is Network, attack complexity is Low, and no privileges or user interaction are required — the combination of factors that produces the highest possible CVSS base scores and the widest practical attack surface.

The vulnerability affects FortiClient EMS versions 7.4.5 and 7.4.6. Version 7.4.7 is the permanent fix, and emergency hotfixes — versions 7.4.5.2111 and 7.4.6.2170 respectively — were released concurrently with the April 4 advisory [1]. The vulnerability was independently discovered by security researchers Simo Kohonen of Defused Cyber and Nguyen Duc Anh, and at least two proof-of-concept exploits had been published to public repositories by the time of disclosure [2].

Exploitation was first observed on watchTowr honeypots on March 31, 2026, coinciding with the Easter holiday weekend — a period of typically reduced security operations staffing — and four days before the public advisory was issued [14].

The Vulnerability Chain: CVE-2026-21643 and CVE-2026-35616

The full scope of the current situation is only visible when the two 2026 vulnerabilities are considered together. CVE-2026-21643, disclosed March 30, 2026, is a SQL injection vulnerability (CWE-89, CVSS 9.8) in FortiClient EMS version 7.4.4 affecting multi-tenant deployments [3]. The flaw is technically similar to CVE-2023-48788 in its class: the HTTP `Site` header, used to identify the tenant context in multi-tenant configurations, is passed directly into a backend PostgreSQL query without sanitization before authentication is enforced. An attacker targeting the `/api/v1/init_consts` endpoint can inject arbitrary SQL and achieve unauthenticated remote code execution. Active exploitation of CVE-2026-21643 was first observed around March 26, 2026 — four days before the public disclosure — and a Shadowserver Foundation scan identified between 2,000 and 2,400 internet-exposed FortiClient EMS instances at risk, with over 1,400 concentrated in the United States and Europe [3, 4, 15].

The patch for CVE-2026-21643 was version 7.4.5. Organizations that followed emergency patching guidance and upgraded their 7.4.4 installations to 7.4.5 within days of the March 30 advisory then found themselves running the version that introduced CVE-2026-35616 — and were exposed to active zero-day exploitation before a patch was available. The back-to-back critical vulnerabilities across consecutive releases raise questions about the depth of security regression testing in Fortinet's release cycle, suggesting the security testing process may not have adequately assessed the API authentication layer when shipping the patch for CVE-2026-21643 [3, 5]. CSO Online has reported that security analyst David Shipley of Beauceron Security characterized CVE-2026-35616 as Fortinet's seventh SQL-related or API-access-control CVE within a twelve-month span — a count that has not been independently audited against primary CVE records but that, if accurate, would point to systemic rather than isolated defects in the product's authentication and input-handling architecture [5].

Exposure Landscape

The attack surface is large enough to cause concern at an industry level. Shodan and Shadowserver Foundation scans placed the population of internet-accessible FortiClient EMS instances at roughly 2,000 to 2,400 prior to the March 30 advisory, before any significant patching activity had occurred [3, 4, 15]. Given the critical severity of CVE-2026-35616, the fact that proof-of-concept code is publicly available, and that exploitation was already observed before the advisory was issued, any organization operating an unpatched FortiClient EMS instance reachable from the public internet, particularly those without continuous monitoring on that host, should treat potential compromise as a working hypothesis pending investigation.

No specific threat actor has been publicly attributed to active exploitation of CVE-2026-35616 or CVE-2026-21643 as of April 5, 2026 [1, 3]. However, the established exploitation playbook from CVE-2023-48788 campaigns — which involved RMM tool deployment, credential theft, and delayed ransomware staging — provides a realistic model for what to anticipate in incident response. The use of legitimate remote management tools during the dwell period makes initial detection particularly difficult, as those tools generate traffic that security controls typically treat as benign.

Recommendations

Immediate Actions

Organizations running FortiClient EMS should treat the following as emergency actions to be completed within 24 to 48 hours. Any FortiClient EMS instance running version 7.4.5 or 7.4.6 should be patched to hotfix version 7.4.5.2111 or 7.4.6.2170 respectively using the official packages from the Fortinet Support Portal, with upgrade to the forthcoming 7.4.7 release as a follow-on action [1]. Organizations still running version 7.4.4 in multi-tenant configurations face a harder decision: upgrading to 7.4.5 resolves CVE-2026-21643 but introduces CVE-2026-35616, and the only complete mitigation path is to apply both the upgrade and the hotfix in a single maintenance window, or to isolate the instance entirely from internet access until 7.4.7 is available.

Where patching cannot be applied immediately, network access to the FortiClient EMS administrative interface should be restricted through firewall rules to known-good management IP ranges. Fortinet's advisory confirms that restricting network access constitutes a valid interim mitigation; there is no workaround that addresses the vulnerability at the application layer without the hotfix [1]. The runZero

fingerprint (`_asset.protocol:http AND protocol:http AND favicon.ico.image.mmh3:=-800551065`) can assist organizations in confirming whether internet-facing assets are running FortiClient EMS [4].

Following any patch activity, organizations should conduct a thorough review of FortiClient EMS access logs for activity prior to the patch date — particularly API calls occurring before authentication would have been enforced. Log retention policies permitting, analysis should extend to at least March 25 to capture the observed pre-disclosure exploitation window. Suspicious API calls, unusual account creation or modification activity, and unexpected changes to endpoint policy configurations are the primary artifacts to hunt.

Short-Term Mitigations

Beyond immediate patching, several architectural controls reduce the ongoing risk from FortiClient EMS exposure. The EMS administrative interface should not be directly reachable from the public internet under any operational model; if remote management is required, access should be gated through a VPN or bastion host with strong multi-factor authentication. Network segmentation that isolates the EMS server from lateral movement paths — particularly preventing outbound connections to arbitrary internet infrastructure from the EMS host itself — limits the blast radius of a successful compromise [7, 8].

Security teams should deploy behavioral monitoring on the FortiClient EMS server host for post-exploitation indicators consistent with those documented in prior campaigns: installation of ScreenConnect, AnyDesk, Atera, or Splashtop agents; execution of Mimikatz or credential harvesting utilities; use of PsExec, WMI-based lateral movement, or Advanced Port Scanner from the host; and anomalous outbound SSL connections to domains with self-signed certificates [6, 7]. Endpoint detection and response (EDR) coverage on the EMS server host itself is essential, as the server's administrative privileges make it an ideal staging post for attackers seeking to propagate through the environment.

Organizations participating in threat intelligence sharing programs should monitor feeds for indicators of compromise associated with CVE-2026-35616 and CVE-2026-21643 campaigns. No attributed threat actor or formal IOC set had been published as of April 5, 2026, but that situation is likely to change rapidly as incident responders begin publishing findings from compromised environments.

Strategic Considerations

The back-to-back critical vulnerabilities in consecutive FortiClient EMS releases raise vendor risk questions that go beyond routine patch management. Organizations with Fortinet as a strategic vendor should formally request a security posture briefing from their Fortinet account team addressing the root cause of the API authentication bypass class of vulnerabilities and the timeline for architectural remediation. CSA's Cloud Controls Matrix mandates formal third-party risk assessment processes, and the recurrence pattern visible in Fortinet's CVE history — particularly across the FortiClient EMS product line — constitutes a material vendor risk signal that merits inclusion in annual supplier reviews [9, 10].

At the architectural level, organizations should examine their dependence on FortiClient EMS as an enforcement point within their Zero Trust architecture. Because FortiClient EMS acts as the policy broker and ZTNA orchestrator for endpoints, its compromise can undermine the integrity of the trust decisions the ZTNA framework is designed to enforce — an attacker who controls EMS can modify compliance posture data, issue rogue configurations to managed endpoints, or suppress security alerts. Zero Trust designs that place excessive trust in the integrity of the EMS control plane without independent verification should be revisited.

CSA Resource Alignment

The FortiClient EMS vulnerability chain intersects directly with several foundational CSA frameworks and guidance documents.

MAESTRO (Agentic AI Threat Modeling): While CVE-2026-35616 is not an AI-specific vulnerability, its exploitation pattern is directly relevant to organizations using AI-driven security orchestration that depends on FortiClient EMS telemetry. MAESTRO Layer 3 (Orchestration and Integration) addresses risks arising from the compromise of orchestration control planes — precisely the role FortiClient EMS plays in a ZTNA deployment. As a hypothetical attack path, an adversary who has corrupted EMS policy data or disabled endpoint compliance enforcement could feed false telemetry into AI-assisted security analysis pipelines, causing those systems to reach incorrect trust decisions. CSA's MAESTRO framework guidance on validating the integrity of data sources feeding AI orchestration layers applies directly here [11].

AI Infrastructure and Cloud Controls Matrix (AICM/CCM): The AICM, as a superset of CCM, addresses infrastructure risk management requirements that extend to third-party security components. CCM control domain TVM-01 (Threat and Vulnerability Management) requires that organizations maintain a continuously updated inventory of known vulnerabilities in their software and infrastructure

components and define SLA-bound remediation timelines tied to CVSS severity. The severity and active-exploitation status of CVE-2026-35616 requires Critical/P1 treatment under most TVM frameworks — a 24-to-72-hour patch SLA for internet-facing instances. CCM IVS-01 (Inventory and Asset Management) is equally relevant: the exposure landscape data suggests that many organizations may not have accurate records of how many FortiClient EMS instances they operate or which are internet-reachable, a prerequisite for effective response [9, 10].

Zero Trust Guidance: CSA's Zero Trust Architecture guidance emphasizes that every component in the trust enforcement chain must itself be protected and monitored; no component, however central, is implicitly trusted. FortiClient EMS functions as a trust broker, and its compromise illustrates the risk of treating enforcement infrastructure as inherently trustworthy. Organizations implementing CSA's Zero Trust principles should apply the same continuous verification posture to their enforcement infrastructure that the architecture requires of endpoints and users [12].

STAR (Security Trust Assurance and Risk): The recurring critical vulnerability pattern in Fortinet FortiClient EMS is the type of systemic vendor security issue that CSA's STAR program is designed to surface through continuous security attestation. Organizations using STAR or CAIQ assessments in their vendor management programs should update their Fortinet assessments to reflect the current CVE chain and require evidence of architectural remediation planning — not merely confirmation that the latest hotfix has been applied [13].

References

[1] Fortinet PSIRT. "FG-IR-26-099: FortiClient EMS – Improper Access Control in API." Fortinet, April 4, 2026.

[2] SecurityOnline.info. "Under Active Attack: Critical 9.1 CVSS FortiClient EMS Flaw (CVE-2026-35616)." SecurityOnline, April 4, 2026.

[3] Help Net Security. "Critical FortiClient EMS Bug Under Active Attack (CVE-2026-21643)." Help Net Security, March 30, 2026.

[4] runZero Research. "Fortinet FortiClient EMS Vulnerability: CVE-2026-35616." runZero, April 2026.

[5] CSO Online. "Fortinet Hit by Another Exploited Cybersecurity Flaw." CSO Online, April 2026.

[6] Darktrace. "FortiClient EMS Exploited: Inside the Attack Chain and Post-Exploitation Tactics (CVE-2023-48788)." Darktrace, 2024.

[7] Kaspersky Securelist. "Patched FortiClient EMS Vulnerability Exploited in the Wild (CVE-2023-48788)." Kaspersky, 2024.

[8] Horizon3.ai. "CVE-2023-48788 FortiClient EMS SQL Injection Deep Dive." Horizon3.ai, 2024.

[9] Cloud Security Alliance. "Cloud Controls Matrix (CCM) v4.0." CSA, 2021.

[10] Cloud Security Alliance. "AI Infrastructure and Cloud Controls Matrix (AICM)." CSA, 2025.

[11] Cloud Security Alliance. "MAESTRO: Agentic AI Threat Modeling Framework." CSA AI Safety Initiative, 2025.

[12] Cloud Security Alliance. "Software Defined Perimeter and Zero Trust." CSA, 2022.

[13] Cloud Security Alliance. "STAR Registry and Continuous Auditing." CSA, 2025.

[14] The Hacker News. "Fortinet Patches Actively Exploited CVE-2026-35616 in FortiClient EMS." The Hacker News, April 2026.

[15] BleepingComputer. "Critical Fortinet FortiClient EMS Flaw Now Exploited in Attacks." BleepingComputer, March 2026.

[16] NIST National Vulnerability Database. "CVE-2023-48788 Detail." NVD, 2024.

[17] CISA. "Known Exploited Vulnerabilities Catalog." CISA, continuously updated.