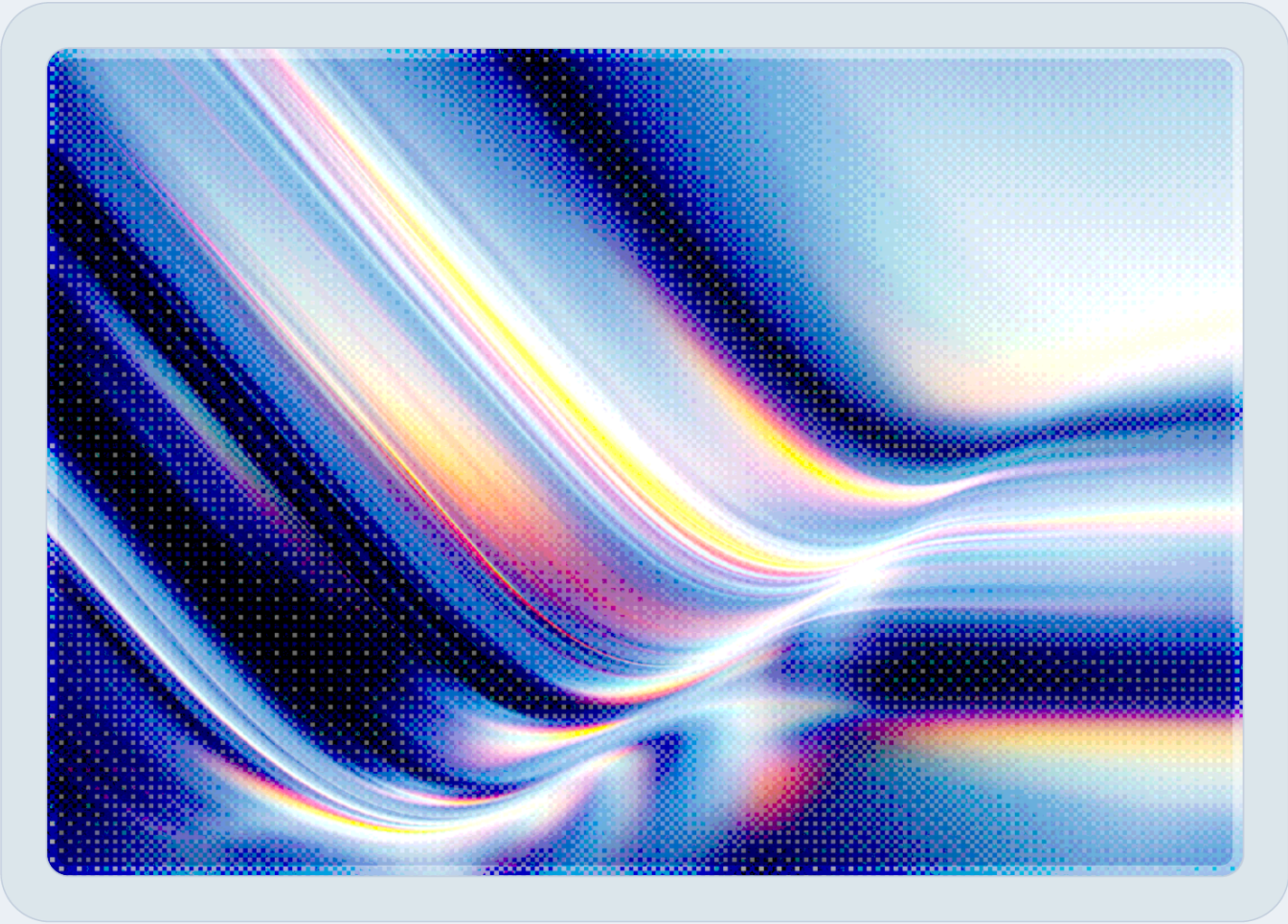
CSAI Foundation | Cloud Security Alliance

Cisco FMC Auth Bypass Exploited to Deploy Qilin Ransomware

2026-09-18

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

Cisco and Cisco Talos have confirmed active, in-the-wild exploitation of two vulnerabilities in Cisco Secure Firewall Management Center (FMC) software: CVE-2026-20079, a maximum-severity (CVSS 10.0) authentication bypass that lets an unauthenticated remote attacker execute scripts and commands as root, and CVE-2026-20316, a lower-severity (CVSS 5.3) flaw involving hardcoded, static credentials for a low-privileged account that becomes dangerous when chained with other FMC weaknesses [1][2][3]. Talos has attributed post-compromise activity on exploited FMC instances to three distinct threat clusters — UAT-12197, which deploys JSP web shells and a Java-based credential harvester; UAT-11823, linked to the Russian state-sponsored group Sandworm, which deploys the Cyclops Blink backdoor; and UAT-11988, a ransomware operation that used stolen FMC access to stage a living-off-the-land intrusion culminating in the deployment of Qilin ransomware [3][4]. CVE-2026-20316 was disclosed and added to the CISA Known Exploited Vulnerabilities (KEV) catalog on July 29, 2026, while CVE-2026-20079 — despite fixes being available since earlier in the year — was confirmed as actively exploited and added to KEV on September 9, 2026, with a federal patch deadline of September 12, 2026 [5][6][7]. As demonstrated in this incident, compromise of a single FMC instance exposed Active Directory service-account credentials, database credentials, and network topology information across the perimeter it managed [3][8], illustrating how one vulnerable management console can become a springboard for ransomware deployment across managed endpoints. No workaround exists for either vulnerability; Cisco's guidance is to apply the available hotfixes immediately and to treat any FMC instance with internet-reachable management interfaces as a priority remediation target [1][9].

Background

Cisco Secure Firewall Management Center is the centralized administration platform for Cisco's Secure Firewall (formerly Firepower) product line, providing a single console through which security teams configure access policies, intrusion prevention rules, and VPN settings across fleets of managed firewall devices [1]. Because FMC holds administrative credentials for every device it manages and aggregates configuration, log, and identity data from across an organization's perimeter, it occupies a position of outsized trust relative to any individual firewall — a compromise of FMC does not just expose one appliance, it can expose the management relationship to all of them. This concentration of trust plausibly explains why FMC has drawn interest from both espionage-motivated state actors and financially

motivated ransomware operators, though the exploitation activity documented by Talos does not by itself establish attacker motive; a similar dynamic has been evident in prior incidents affecting Cisco's SD-WAN management plane and Palo Alto Networks' GlobalProtect infrastructure [10][11].

CVE-2026-20079 stems from an improper system process that Cisco says is created at boot time on unpatched FMC instances. According to Cisco's advisory, a startup process establishes a partial authentication session in the underlying `sfsnort.sessions` database; if no legitimate user authenticates to the device immediately after boot, that partial session persists and can be manipulated by a remote attacker into functioning credentials, at which point the attacker can invoke a broad set of CGI scripts on the web interface without ever supplying valid authentication [1][2]. Because the flaw requires only that an attacker send specially crafted HTTP requests to the FMC web interface, and no user interaction, valid credentials, or prior access is needed, it carries the maximum CVSS 3.1 base score of 10.0 [1]. CVE-2026-20316, by contrast, involves a static, low-privileged account with credentials effectively hardcoded into the software; on its own, the account allows only limited access, but Cisco and Talos have both noted that it can be combined with other FMC weaknesses to escalate privileges or, as observed in the wild, used directly as an initial-access foothold for reconnaissance [3][8].

The two vulnerabilities followed different disclosure paths. CVE-2026-20316 was disclosed and immediately flagged as exploited, with CISA adding it to the KEV catalog on the same day, July 29, 2026 [5][8]. CVE-2026-20079 had fixed software releases available earlier in 2026 but was not confirmed as actively exploited until Cisco's PSIRT and Cisco Talos identified in-the-wild abuse in August and September 2026; CISA subsequently added it to the KEV catalog on September 9, 2026, alongside three other actively exploited vulnerabilities, with a compressed federal remediation deadline of September 12, 2026 [6][7][9]. Cisco has stated that it is preparing a comprehensive hardening release that combines both hotfixes with additional internally discovered fixes, distinct from the emergency patches already available for each individual flaw [3].

Security Analysis

Talos's investigation into ongoing FMC exploitation identified three distinct threat clusters operating against compromised instances, each with a different objective and toolset. The first, tracked as UAT-12197, focuses on credential theft: after gaining access, it deploys JSP web shells into the FMC's Tomcat application directory and installs a Java archive file that functions as a command executor, which it then uses to query internal databases and extract stored authentication credentials [3][4]. The second cluster, UAT-11823, has been linked by Talos to the Russian state-sponsored group Sandworm and pursues a more persistent, espionage-oriented objective: it establishes Netcat reverse shells, in some cases by modifying the `license.tmp` file to trigger command execution, harvests configuration data

from every device the compromised FMC manages, and ultimately deploys a variant of the Cyclops Blink malware family — a modular backdoor previously associated with Sandworm's targeting of network edge devices — to maintain long-term access [3][4].

The third cluster, UAT-11988, is the one responsible for the Qilin ransomware deployments that give this incident its most immediate operational urgency. Unlike the other two clusters, UAT-11988 relies primarily on CVE-2026-20316's static credentials for initial access rather than the more severe CVE-2026-20079 authentication bypass, then pivots to a living-off-the-land approach that minimizes the deployment of custom malware in favor of abusing legitimate FMC tooling — including the built-in `package_info.pl` utility — for reconnaissance [3][4]. From that foothold, the group collected an unusually complete inventory of the target environment: hostnames, IP addresses, directory listings, Active Directory service-account credentials, MySQL database credentials, domain account information, and mappings between internal server hostnames and IP addresses, all information that would ordinarily require far deeper network penetration to assemble [3][4]. The group then established SOCKS5 proxies and reverse SSH tunnels to forward LDAP, Kerberos, and SMB traffic out through the compromised FMC instance, used post-exploitation frameworks including Impacket and Invoke-TheHash to move laterally using the harvested credentials, deployed tools designed to disable endpoint detection and response agents, and ultimately executed Qilin ransomware against selected systems within the environment [3][4].

This attack chain illustrates a pattern that distinguishes FMC compromise from a typical single-endpoint ransomware intrusion: because FMC's function is to manage security policy and credentials across an organization's entire firewall fleet, a single authentication bypass on the management console yielded the reconnaissance depth — domain credentials, internal topology, service account details — that ransomware operators would otherwise need to build incrementally through conventional lateral movement, a process that typically requires substantially more time and operational risk. The management plane, in effect, did the attacker's reconnaissance work for them. This also means that organizations evaluating their exposure should not treat FMC compromise as a contained incident affecting only the management appliance; any credentials or configuration data the FMC instance had visibility into should be considered potentially exposed, and downstream managed firewalls, VPN configurations, and any directory-integrated authentication should be reviewed for signs of misuse.

Cisco's guidance identifies a detectable artifact of exploitation: suspicious log entries referencing `/var/tmp/license.tmp` in FMC syslog output may indicate exploitation attempts tied to the license-file manipulation technique observed with UAT-11823's activity, and Talos has published Snort detection rules (signature IDs in the 66075–66080 range for CVE-2026-20079, 66883 for CVE-2026-20316, and 66960–66961 for associated malware) that organizations running Cisco's intrusion prevention capability should ensure are enabled [2][3]. Because three separate threat clusters — with three different objectives, ranging from credential harvesting to state-sponsored persistence to

ransomware deployment — are exploiting these vulnerabilities concurrently, organizations should not assume that patching alone resolves the incident if compromise has already occurred; each cluster leaves distinct artifacts that require separate investigation.

Recommendations

Immediate Actions

Organizations running Cisco Secure FMC should confirm their current software version against Cisco's fixed-release table and apply the available hotfixes for both CVE-2026-20079 and CVE-2026-20316 without delay, treating this as an emergency change given confirmed active exploitation by multiple independent threat actors [1][9]. Security teams should audit FMC syslog data for suspicious references to `/var/tmp/license.tmp`, review Tomcat application directories for unauthorized JSP files or unexpected Java archives, and verify that Talos's published Snort signatures for both CVEs are active on any Cisco intrusion prevention sensors monitoring FMC traffic [2][3]. Any organization that identifies indicators of compromise, or that cannot rule out prior exploitation given the vulnerabilities' extended pre-disclosure exploitation windows, should treat the incident as a potential credential-exposure event across the entire fleet of firewalls the affected FMC instance manages — not merely a compromise of the management appliance itself — and begin rotating Active Directory service-account, database, and administrative credentials that the FMC instance had access to [3][4].

Short-Term Mitigations

Because no configuration-based workaround exists for either vulnerability, organizations unable to patch immediately should restrict internet accessibility to FMC management interfaces as an interim risk-reduction measure, limiting reachability to a small set of trusted administrative network segments [3][9]. Given that UAT-11988's ransomware deployment relied heavily on SOCKS5 proxies and reverse SSH tunnels established through the compromised FMC to reach internal LDAP, Kerberos, and SMB services, organizations should also review firewall and network flow logs for anomalous outbound tunneling activity originating from FMC management addresses, and ensure that FMC management network segments are not permitted broad outbound connectivity to internal identity and file-sharing infrastructure by default [4]. Organizations should plan to apply Cisco's forthcoming comprehensive hardening release, which combines both hotfixes with additional internally discovered fixes, once it becomes available, rather than treating the individual emergency hotfixes as a permanent end state [3].

Strategic Considerations

This incident is the latest in a recurring pattern of actively exploited authentication bypasses affecting the centralized management planes of major network security vendors' products, following closely on prior widely exploited flaws in Cisco's SD-WAN management infrastructure and Palo Alto Networks' GlobalProtect remote-access platform [10][11]. Organizations with significant investment in centralized firewall or network management consoles should evaluate whether those consoles are architected under zero trust principles — with network segmentation isolating management interfaces from both the internet and general internal network segments, continuous monitoring of management-plane activity independent of the console's own logs, and credential scoping that limits the blast radius of any single management system's compromise — rather than being implicitly trusted as a secure administrative enclave. The fact that three independent threat clusters with entirely different objectives converged on the same two vulnerabilities within weeks of active exploitation being confirmed also suggests that disclosed authentication bypasses in centralized network-management infrastructure carry an elevated likelihood of rapid multi-actor exploitation, and patch prioritization processes should account for this risk rather than treating such flaws as a niche concern affecting only sophisticated adversaries.

CSA Resource Alignment

This incident extends a pattern evident across 2026 in authentication bypass and management-plane compromise vulnerabilities affecting the centralized consoles that govern network security infrastructure. The pre-disclosure exploitation of Cisco's Catalyst SD-WAN Manager under CVE-2026-20245 [10] presents a structurally similar case, in which attackers achieved root-level compromise of a Cisco management-plane product months before a patch was available; the same priorities that applied there — segmenting management interfaces from general network access and preserving forensic evidence before remediation — apply directly to organizations investigating potential FMC compromise here. The actively exploited PAN-OS GlobalProtect authentication bypass, CVE-2026-0257 [11], reached a similar structural conclusion in a competing vendor's product: internet-exposed network security management interfaces represent a disproportionately high-value target because of the elevated privileges and broad visibility they hold, and multiple intrusions traced to that vulnerability likewise culminated in Qilin ransomware deployment, a monetization path consistent with what Talos observed from UAT-11988's use of FMC-derived credentials. The FortiBleed campaign against internet-facing FortiGate firewalls [12] documented a separate case in which compromised firewall management functionality was repurposed for large-scale credential harvesting later fed into ransomware operations. Taken together, these incidents suggest that the identity and access management principles reflected in the CSA AI Controls Matrix (AICM) v1.1's IAM domain [13] — which, while developed for AI system

contexts, address credential lifecycle management and privileged access to administrative interfaces in terms applicable here — offer a relevant control baseline for organizations seeking to reduce the risk that a single management-plane compromise cascades into fleet-wide credential exposure and ransomware deployment.

References

[1] Cisco. "Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability." Cisco Security Advisories, updated September 16, 2026.

[2] VulnCheck. "CVE-2026-20079 - Cisco FMC Authentication Bypass RCE Analysis." VulnCheck, September 2026.

[3] Cisco Talos. "Active exploitation of Cisco Secure Firewall Management Center vulnerabilities." Cisco Talos Blog, September 9, 2026.

[4] The Hacker News. "Cisco FMC Flaws Exploited to Steal Credentials and Deploy Qilin Ransomware." The Hacker News, September 2026.

[5] Cybersecurity and Infrastructure Security Agency. "CISA Adds One Known Exploited Vulnerability to Catalog." CISA, July 29, 2026.

[6] BleepingComputer. "Cisco confirms CVE-2026-20079 Secure FMC flaw exploited in attacks." BleepingComputer, September 2026.

[7] Cybersecurity and Infrastructure Security Agency. "CISA Adds Four Known Exploited Vulnerabilities to Catalog." CISA, September 9, 2026.

[8] Help Net Security. "Cisco FMC static credentials exploited by attackers (CVE-2026-20316)." Help Net Security, July 30, 2026.

[9] Help Net Security. "Cisco FMC bugs exploited by nation-state and ransomware actors (CVE-2026-20079, CVE-2026-20316)." Help Net Security, September 10, 2026.

[10] The Hacker News. "Cisco Catalyst SD-WAN Zero-Day CVE-2026-20245 Exploited to Gain Root Access." The Hacker News, June 2026.

[11] The Hacker News. "PAN-OS GlobalProtect Authentication Bypass (CVE-2026-0257) Under Active Exploitation." The Hacker News, May 2026.

[12] The Hacker News. "FortiBleed Targeted FortiGate Firewalls in 110 Million-Credential Harvesting Operation." The Hacker News, June 2026.

[13] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance.