Interlock Ransomware Weaponizes Cisco FMC Zero-Day

CVE-2026-20131 and the Ransomware-as-Zero-Day-Holder Threat Model

Unofficial AI-assisted Research

Cloud Security Alliance AI Safety Initiative

2026-03-19

Key Takeaways

- Interlock ransomware exploited CVE-2026-20131, a CVSS 10.0 unauthenticated remote code execution (RCE) vulnerability in the Cisco Secure Firewall Management Center (FMC) web management interface, for 37 days before Cisco released a patch on March 4, 2026, and 51 days before public disclosure on March 18, 2026 [1][2].
- The vulnerability stems from insecure deserialization of Java byte streams, permitting unauthenticated attackers to achieve root-level command execution on the underlying Linux OS of the FMC appliance — the centralized management plane for Cisco Firepower perimeter defense appliances [1][3].
- All organizations running on-premises Cisco FMC versions in the affected ranges should treat patching as an emergency priority; no workaround exists [1][2].
- Interlock's exploitation of CVE-2026-20131 exemplifies an emerging threat model: ransomware groups acquiring or independently discovering zero-day exploits to target high-privilege network management infrastructure, a pattern also established by Cl0p, Black Basta, and BianLian [4][5][6].
- A companion vulnerability, CVE-2026-20079 (authentication bypass in the FMC web interface, also CVSS 10.0), affects the same version ranges and was patched simultaneously; organizations should assess both [2][7].

Background

Interlock Ransomware: From Opportunist to Zero-Day Holder

Interlock ransomware was first identified in late September 2024 by Forescout's Vedere Labs, initially tracked under the codename "Chaya_002" [8]. Interlock, initially observed using drive-by downloads and purchased Initial Access Broker credentials [8], has demonstrated increasing operational sophistication, culminating in the acquisition and weaponization of an unpatched enterprise vulnerability against high-privilege network infrastructure.

By early 2026, Interlock had claimed more than 60 victims, with over 50 of those compromises occurring during 2025 alone [8][9]. The group's targeting has remained concentrated in sectors where operational disruption produces maximum leverage: healthcare, municipal government, and manufacturing. Notable victims include DaVita (a kidney dialysis provider whose March 2025 compromise resulted in approximately 941 GB of patient data exfiltrated and an estimated 2.4 to 2.7 million individuals affected), Kettering Health in Ohio (May 2025, which led to canceled chemotherapy and pre-surgery appointments), and the City of Saint Paul, Minnesota (July 2025, prompting Governor Tim Walz to activate the National Guard and a local emergency declaration) [10][11][12].

The FBI, CISA, HHS, and MS-ISAC issued a joint advisory (AA25-203A) in July 2025 detailing Interlock's known indicators of compromise and tactics, techniques, and procedures [9]. Even so, the group continued to escalate its capabilities. By January 2026, Interlock had crossed a threshold that relatively few financially motivated criminal organizations have reached: independent or brokered zero-day exploitation of enterprise network security infrastructure.

CVE-2026-20131: A Maximum-Severity Deserialization Flaw in Cisco FMC

Cisco Secure Firewall Management Center (FMC), deployed on-premises, serves as the centralized command plane for Cisco Firepower threat defense appliances. It aggregates policy management, traffic logs, network topology data, and access control rules for an organization's Cisco-managed network perimeter. This architectural role — managing the devices that defend the network — makes it a high-value target: compromising the FMC does not merely breach one system; it grants an attacker visibility into, and potential control over, the security posture of all managed Cisco Firepower devices.

CVE-2026-20131 is an insecure deserialization vulnerability (CWE-502: Deserialization of Untrusted Data) affecting the web-based management interface of Cisco Secure FMC Software in on-premises deployments [1][2][3]. The interface accepts serialized Java objects from unauthenticated sources without enforcing class allowlisting prior to deserialization. An attacker can send a crafted HTTP POST request containing a malicious serialized Java payload — identifiable by the Java magic bytes `0xAC ED 00 05` — paired with gadget chains such as those in Apache Commons Collections, triggering arbitrary command execution as root on the FMC's underlying Linux operating system [3][7].

The vulnerability carries a CVSS v3.1 score of 10.0 (Critical), with an attack vector of Network, attack complexity Low, no privileges required, no user interaction, changed scope, and High impact across confidentiality, integrity, and availability [1][2]. Cisco confirmed there are no workarounds; the only remediation is upgrading to a fixed software version [1]. Cloud-Delivered FMC, Cisco ASA, Cisco FTD, and Security Cloud Control are not affected [1].

Affected version ranges span the substantial installed base across FMC 6.4.0.13 through versions prior to the fixed releases in each branch (7.0.9, 7.2.11, 7.4.6, 7.6.5, 7.7.12, and 10.0.1) [1][2]. Cisco assigned Bug ID CSCwt14636 and published advisory cisco-sa-fmc-rce-NKhnULJh [1].

Security Analysis

The Exploitation Timeline: 51 Days of Silent Risk

Interlock began exploiting CVE-2026-20131 as a zero-day on January 26, 2026 — a full 37 days before Cisco released the patch on March 4, 2026, and 51 days before public disclosure on March 18, 2026 [1][2][13]. During this window, affected organizations had no vendor-supplied remediation and no public awareness that their FMC infrastructure was under active attack.

Amazon's MadPot honeypot network independently detected exploitation traffic linked to Interlock's infrastructure and, following discovery of a misconfigured Interlock server, recovered and analyzed the group's attack toolkit as deployed in this campaign [13]. This discovery appears to have contributed to the security community's understanding of the attack chain, and may have informed Cisco's disclosure process.

The FMC Attack Chain in Detail

Interlock's exploitation of CVE-2026-20131 represents a methodical multi-stage intrusion that begins at the FMC management interface and terminates in ransomware deployment across Windows, Linux, and VMware ESXi targets. Understanding the sequence is critical for defenders assessing exposure and designing detection logic.

The initial exploitation phase involves crafted HTTP requests to the FMC web management interface carrying malicious serialized Java objects. Successful exploitation is confirmed by an outbound HTTP PUT request from the victim FMC to attacker-controlled infrastructure — a callback mechanism that also serves as a beacon for the attacker and, critically, as an observable indicator of compromise for network defenders [13]. Root-level ELF binaries are then downloaded and executed on the FMC's Linux base.

From this foothold, Interlock deploys a suite of post-exploitation tooling. Custom JavaScript and Java remote access trojans provide persistent shell access, file transfer, and SOCKS5 proxy capabilities. Bash scripts configure the compromised FMC as an HTTP reverse proxy using HAProxy on port 80, with log

wiping via cron jobs to inhibit forensic investigation [9][13]. Memory-resident webshells maintain persistence between reboots and decrypt and execute subsequent command payloads.

Lateral movement pivots on the FMC's inherent network visibility. Because the FMC maintains authenticated relationships with all managed Firepower devices, and because it aggregates routing data, access control policy, and traffic logs, an attacker with root on the FMC possesses a strategic reconnaissance platform that is largely invisible to the devices it manages in environments where the FMC is the primary aggregation point for security telemetry. Interlock pairs this with ConnectWise ScreenConnect for durable remote access, Certify (an offensive Active Directory Certificate Services tool) for AD privilege escalation through misconfigured certificate templates, and AzCopy for bulk exfiltration of data to Azure Blob Storage — a Microsoft-signed binary that many DLP and egress controls do not flag [9][13].

Data exfiltration, which typically precedes encryption by 72 to 96 hours, leverages the FMC's network positioning to identify and reach high-value data stores that might otherwise be isolated behind the firewall perimeter [9]. Ransomware encryptors are then deployed enterprise-wide, with ransom notes distributed via Group Policy Objects to maximize reach.

The Ransomware-as-Zero-Day-Holder Threat Model

CVE-2026-20131 is not an anomaly in Interlock's trajectory; it is consistent with a documented pattern in the ransomware ecosystem. Financially motivated criminal groups increasingly acquire, develop, or barter for unpatched vulnerabilities targeting enterprise-grade network and security infrastructure, and then exploit those vulnerabilities at scale before patches and public disclosure narrow the opportunity window.

Cl0p (also tracked as TA505 or Snakefly) has most thoroughly institutionalized this model. The group's sequential exploitation of Accellion FTA (CVE-2020-12271), Fortra GoAnywhere MFT (CVE-2023-0669), and MOVEit Transfer (CVE-2023-34362) demonstrated a repeatable playbook: acquire a zero-day against a widely deployed file transfer or management platform, deploy it silently across thousands of organizations, exfiltrate data, and then activate extortion demands simultaneously [4][5]. The MOVEit campaign alone compromised an estimated 2,000 or more organizations during summer 2023 [4]. In 2025, Cl0p continued this pattern with CVE-2025-61882, a critical vulnerability in Oracle E-Business Suite that the group exploited prior to patching [17].

Other groups have moved in the same direction. Leaked Black Basta operational chat logs revealed the group was offered a zero-day for Ivanti Connect Secure for $200,000 and separately explored a Juniper SRX firewall zero-day — ultimately set aside due to operational complexity — as a potential attack

primitive [6]. BianLian and RansomEXX jointly exploited CVE-2025-31324 (SAP NetWeaver) as a zero-day for webshell deployment [6]. Play ransomware exploited CVE-2025-29824 in the Windows CLFS driver before a patch was available [6].

Ransomware operators face increasing friction from law enforcement disruptions, cryptocurrency tracking, and improved endpoint detection. Zero-day exploits against network management infrastructure offer a counterbalancing advantage: they provide initial access before defenders can prepare, and they target the infrastructure layer that security operations centers rely on for visibility, creating a compound defensive gap. According to VulnCheck analysis, 56.4% of ransomware-related CVEs disclosed in 2025 were first identified through zero-day exploitation by financially motivated actors, up from 33% in 2024 [16].

The practical implication is that organizations should no longer treat zero-day exposure as a nation-state-only risk. Network management consoles, file transfer appliances, backup systems, and identity platforms are now primary targets for criminal ransomware groups with the resources and operational sophistication to acquire or develop pre-patch exploits.

Recommendations

Immediate Actions

Organizations running on-premises Cisco Secure FMC should treat patch deployment as an emergency response, not a routine maintenance item. Cisco's patches released on March 4, 2026 address CVE-2026-20131 and CVE-2026-20079; both vulnerabilities carry a CVSS score of 10.0 and have been confirmed under active exploitation [1][2]. Given the 37-day gap between first exploitation and the patch release, and the 51-day gap to public disclosure, organizations should also conduct retrospective investigation of FMC logs for indicators consistent with exploitation — specifically, unexpected outbound HTTP PUT connections from the FMC management interface to external IP addresses, presence of Java magic bytes (`0xAC ED 00 05`) in web server logs, unexpected ELF binary downloads, and cron-scheduled log deletion activity [13].

For Qualys users, QIDs 317769 and 317770 provide automated detection for CVE-2026-20079 and CVE-2026-20131 respectively [7]. Arctic Wolf and CyCognito have published threat detection content for both CVEs as of March 2026 [2][15]; Securonix has separately documented Interlock ransomware TTPs in a related campaign analysis [14].

Organizations should also audit their AzCopy usage patterns. Interlock's documented use of AzCopy for bulk exfiltration to Azure Blob Storage — exploiting the binary's Microsoft-signed status — means that egress monitoring for AzCopy invocations with external destination accounts, particularly in contexts where AzCopy was not previously present on a system, is a high-signal detection opportunity.

Short-Term Mitigations

While patching proceeds, organizations should evaluate whether FMC management interfaces are exposed to any network segment other than a dedicated, restricted management network. Cisco notes that restricting management interface access to non-internet-facing networks reduces attack surface [1]. Although this does not eliminate risk from a threat actor with internal network access, it reduces the unauthenticated remote exploitation surface that Interlock exploited.

Organizations should review and harden Active Directory Certificate Services configurations, as Interlock's documented use of Certify indicates that misconfigured AD CS templates are a consistent escalation path post-FMC compromise. The guidance in Microsoft's May 2022 advisory on AD CS misconfigurations (ESC1 through ESC8 templates) remains applicable [9][18].

Defenders should also implement anomaly detection for remote management tools deployed outside standard change control. Interlock's persistent use of ConnectWise ScreenConnect — including cracked versions — as a post-exploitation persistence mechanism means that unexpected ScreenConnect installations, particularly on server infrastructure, warrant immediate investigation [9].

Strategic Considerations

The Interlock FMC campaign illustrates why security management infrastructure must be governed under the same — or stricter — security controls as the assets it protects. Organizations that segment and harden endpoints and cloud workloads while leaving network management consoles with broad access and relaxed monitoring posture have an inverted risk model: the attacker will compromise the management plane to bypass endpoint defenses, not the other way around. Network operations centers, security operations platforms, and backup infrastructure require explicit threat modeling and adversarial testing.

More broadly, organizations should evaluate their ransomware defenses against the zero-day-holder threat model rather than assuming that timely patching is sufficient protection. Because exploitation precedes disclosure in this model, patch cadence is a lagging control. Leading controls — network segmentation, privileged access workstations for management console access, behavioral anomaly detection on management plane traffic, and zero trust enforcement at the management interface layer — provide protective value independent of patch timing.

Finally, organizations with meaningful Cisco FMC deployments should validate their incident response procedures include playbooks for management infrastructure compromise. The distinctive forensic signatures of this campaign (Java deserialization artifacts in web logs, AzCopy exfiltration telemetry, HAProxy-on-80 reverse proxy configuration) provide actionable detection and response anchors that IR teams should encode into runbooks before the next exploitation campaign requires them.

CSA Resource Alignment

This advisory connects directly to multiple CSA frameworks and publications that provide structural guidance for organizations seeking to reduce their exposure to the threat patterns Interlock's FMC campaign exemplifies.

The FMC compromise parallels the CSA MAESTRO framework's concerns about Layer 4 (Execution and Observation) and Layer 5 (Communication and Coordination) integrity — an attacker controlling the FMC gains the same compound visibility and control advantages that MAESTRO attributes to compromised AI agent orchestrators, applied here at the network security layer. MAESTRO's guidance on protecting management plane integrity is directly applicable.

The CSA AI Infrastructure Controls Matrix (AICM), as a superset of the Cloud Controls Matrix (CCM), provides control mappings for vulnerability management (VM-01 through VM-06), incident response (SEF-01 through SEF-08), and network security (IVS controls) that are directly responsive to the failure modes this campaign exploits. CCM control IVS-04 (Network Security), IVS-09 (Network Defense), and VM-06 (Patch Management) in particular provide baseline standards against which affected organizations can benchmark their current posture.

CSA's published guidance on Zero Trust architecture speaks directly to the access model failures that enabled this campaign. Management interfaces for network security infrastructure should operate under zero trust assumptions — requiring explicit, context-aware authentication and authorization for every management session regardless of network location — rather than implicit trust based on network segment membership.

The CSA Security Trust Assurance and Risk (STAR) program offers organizations a structured mechanism for assessing vendor security posture, including the patch disclosure practices that shaped the 51-day gap between Interlock's first exploitation of CVE-2026-20131 and public disclosure. Organizations that depend on Cisco FMC and similar management infrastructure may wish to use STAR-aligned assessments to establish contractual expectations around coordinated vulnerability disclosure timelines and customer notification.

CSA's prior research notes on the FortiGate NGFW credential theft campaign (March 2026) and AI-assisted network device mass exploitation (March 2026) provide companion analysis of the broader trend toward ransomware and criminal actors targeting network perimeter and management infrastructure as a primary intrusion vector. Collectively these incidents support a threat modeling posture that treats all network management infrastructure as high-value adversarial targets, not as trusted backstops.

References

[1] Cisco Systems, "Cisco Secure Firewall Management Center Software Remote Code Execution Vulnerability," Advisory cisco-sa-fmc-rce-NKhnULJh, March 18, 2026. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh

[2] Arctic Wolf, "CVE-2026-20079 and CVE-2026-20131: Maximum-Severity Vulnerabilities in Cisco FMC," March 2026. https://arcticwolf.com/resources/blog-uk/cve-2026-20079-cve-2026-20131-maximum-severity-vulnerabilities-in-cisco-fmc/

[3] CVEReports, "CVE-2026-20131: Unauthenticated RCE in Cisco Secure FMC via Java Deserialization," March 2026. https://cvereports.com/reports/CVE-2026-20131

[4] CISA, "CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability," Advisory AA23-158A, June 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

[5] Akamai, "MOVEit SQL Injection Zero-Day Exploited by CL0P Ransomware Group," June 2023. https://www.akamai.com/blog/security-research/moveit-sqli-zero-day-exploit-clop-ransomware

[6] Outpost24, "Lessons From 2025: Zero-Day Exploitation Shaping 2026," January 2026. https://outpost24.com/blog/top-zero-day-exploits-2025/

[7] Qualys ThreatPROTECT, "Cisco Patches Secure Firewall Management Center Software Vulnerabilities (CVE-2026-20079, CVE-2026-20131)," March 5, 2026. https://threatprotect.qualys.com/2026/03/05/cisco-patches-secure-firewall-management-center-software-vulnerabilities-cve-2026-20079-cve-2026-20131/

[8] Forescout Vedere Labs, "A Year Later, Interlock Ransomware Keeps Leveling Up," October 2025. https://www.forescout.com/blog/a-year-later-interlock-ransomware-keeps-leveling-up/

[9] CISA/FBI/HHS/MS-ISAC, "#StopRansomware: Interlock," Joint Advisory AA25-203A, July 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-203a

[10] The Register, "DaVita Tells 2.4M People Ransomware Scum Stole Health Data," August 2025. https://www.theregister.com/2025/08/22/davita_ransomware_infection/

[11] Kettering Health, "Cybersecurity Incident FAQ," May 2025. https://ketteringhealth.org/cybersecurity-incident-faq/

[12] BleepingComputer, "Saint Paul Cyberattack Linked to Interlock Ransomware Gang," July 2025. https://www.bleepingcomputer.com/news/security/saint-paul-cyberattack-linked-to-interlock-ransomware-gang/

[13] AWS Security Blog, "Amazon Threat Intelligence Teams Identify Interlock Ransomware Campaign Targeting Enterprise Firewalls," March 2026. https://aws.amazon.com/blogs/security/amazon-threat-intelligence-teams-identify-interlock-ransomware-campaign-targeting-enterprise-firewalls/

[14] Securonix, "CVE-2025-61155 and Interlock Ransomware: A Converging Threat," 2026. https://connect.securonix.com/threat-research-intelligence-62/cve-2025-61155-and-interlock-ransomware-a-converging-threat-198

[15] CyCognito, "Emerging Threat: Cisco Secure Firewall Management Center Root Compromise (CVE-2026-20079, CVE-2026-20131)," March 2026. https://www.cycognito.com/blog/emerging-threat-cisco-secure-firewall-management-center-root-compromise-cve-2026-20079-cve-2026-20131/

[16] VulnCheck, "2026 Exploit Intelligence Report," January 2026. https://vulncheck.com/reports/exploit-intelligence-2026

[17] CISA Known Exploited Vulnerabilities Catalog, "CVE-2025-61882: Oracle E-Business Suite Unspecified Vulnerability," added October 6, 2025. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[18] SpecterOps, "Certified Pre-Owned: Abusing Active Directory Certificate Services," Will Schroeder and Lee Christensen, May 2022. https://posts.specterops.io/certified-pre-owned-d95910965cd2