Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-20131: Interlock Ransomware Exploits Critical Cisco Secure FMC Flaw

Date of Publication	Admiralty Code	TA Number
March 20, 2026	A1	TA2026079

Summary

First Seen: January 26, 2026
Affected Products: Cisco Secure Firewall Management Center (FMC) Software, Cisco Security Cloud Control (SCC) Firewall Management
Malware: Interlock Ransomware Group
Targeted Industries: Education, Engineering, Architecture and Construction, Manufacturing, Healthcare, and Government sectors
Impact: CVE-2026-20131 is a critical remote code execution vulnerability (CVSS 10.0) in Cisco Secure Firewall Management Center (FMC) that allows an unauthenticated attacker to execute arbitrary Java code as root via insecure deserialization in the web management interface. The Interlock ransomware group has been actively exploiting this flaw as a zero-day since January 26, 2026, more than a month before Cisco's public disclosure on March 4, 2026. Their exposed toolkit reveals a sophisticated multi-stage attack chain including custom RATs, memory-resident web shells, and infrastructure laundering capabilities targeting education, engineering, healthcare, and government sectors. No workarounds are available, and users are strongly urged to apply Cisco's security patches immediately.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-20131	Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management Deserialization of Untrusted Data Vulnerability	Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management	✓	✓	✓
CVE-2026-20079	Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability	Cisco Secure Firewall Management Center Software	✗	✗	✓

Note: CVE-2026-20131- Exploitation occurred before the patch, but was only discovered after the patch was already available.

Vulnerability Details

#1

CVE-2026-20131 is a critical remote code execution vulnerability in Cisco Secure Firewall Management Center (FMC) Software. The flaw exists in the web-based management interface, where an unauthenticated, remote attacker can send a crafted serialized Java object that the server processes without proper validation, granting arbitrary Java code execution as root, achieving complete system compromise. Disclosed by Cisco on March 4, 2026, alongside CVE-2026-20079, the vulnerability affects both on-premises FMC Software and SaaS-delivered Cisco Security Cloud Control (SCC) Firewall Management, while ASA and FTD Software remain unaffected. No workarounds are available.

#2

Threat intelligence analysis confirmed that the Interlock ransomware group exploited CVE-2026-20131 as a zero-day since January 26, 2026, more than a month before public disclosure. A misconfigured Interlock infrastructure server exposed their complete toolkit, revealing a multi-stage attack chain with custom remote access trojans, reconnaissance scripts, infrastructure laundering mechanisms, and evasion techniques. These findings were shared with Cisco, which subsequently confirmed active exploitation.

#3

The attack chain delivers malicious serialized Java objects to the FMC management interface via crafted HTTP requests. Upon exploitation, the compromised system confirms success via an HTTP PUT request to attacker infrastructure, then fetches additional payloads including ELF binaries. Interlock's toolkit includes custom JavaScript and Java RATs using RC4-encrypted WebSocket connections, a memory-resident Java web shell evading file-based detection, PowerShell reconnaissance scripts, and infrastructure laundering scripts configuring disposable reverse proxies with log erasure every five minutes. They also abuse ConnectWise ScreenConnect for persistent access, Certify for AD CS exploitation, and Volatility for credential extraction from memory dumps.

#4

Interlock targets education, engineering, architecture and construction, manufacturing, healthcare, and government sectors where operational disruption maximizes payment pressure. Their extortion combines data encryption with regulatory exposure threats, using per-victim identifiers embedded in ransom notes. Users should immediately apply Cisco's patches, review logs for published indicators of compromise, audit for unauthorized ScreenConnect installations, restrict FMC management interface exposure, and implement defense-in-depth strategies.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-20131	Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management	cpe:2.3:a:cisco:secure_firewall_management_center:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:security_cloud_control:*:*:*:*:*:*:*:*	CWE-502
CVE-2026-20079	Cisco Secure Firewall Management Center (FMC) Software	cpe:2.3:a:cisco:secure_firewall_management_center:*:*:*:*:*:*:*:*	CWE-288

Recommendations

Apply Cisco Security Patches Immediately: Organizations running Cisco Secure Firewall Management Center should immediately apply the fixed software releases provided by Cisco. Use Cisco's Software Checker tool to identify the appropriate fixed release for your deployment. For Cisco Security Cloud Control (SCC) Firewall Management users, no action is required as the SaaS offering is upgraded by Cisco as part of maintenance. Patching is the most effective remediation for this critical vulnerability and should be treated as an emergency priority.

Conduct Compromise Assessment and Log Review: Given that active exploitation has been ongoing since at least January 26, 2026, organizations should conduct thorough security assessments to determine whether their environments have been compromised. Review network and system logs for the indicators of compromise including the exploit source IPs (206[.]251[.]239[.]164, 199[.]217[.]98[.]153, 89[.]46[.]237[.]33), C2 domains (browser-updater[.]click, os-update-server[.]com and related variants), and the specific HTTP User-Agent string and TLS JA3/JA4 fingerprints associated with the exploit traffic.

Audit Remote Access Tool Deployments: Review all ConnectWise ScreenConnect installations across the environment for unauthorized deployments, as the Interlock group deploys legitimate remote access tools alongside custom implants to maintain redundant access. Any ScreenConnect instance that cannot be attributed to authorized IT operations should be investigated immediately and isolated pending forensic analysis.

Restrict Management Interface Exposure: Ensure that the FMC web-based management interface is not directly accessible from the public internet. Implement network segmentation and access control lists to restrict management interface access to trusted administrative networks only. While this does not eliminate the vulnerability, it significantly reduces the attack surface available to remote adversaries.

Strengthen Defense-in-Depth Posture: Implement layered security controls to ensure that no single point of failure leaves the organization defenseless. This includes deploying network segmentation to limit lateral movement, maintaining up-to-date endpoint detection and response (EDR) solutions, enabling multi-factor authentication on all administrative interfaces, conducting regular vulnerability scans, and testing incident response procedures specifically for ransomware scenarios. Defense-in-depth is essential for protecting against zero-day exploits during the window between initial exploitation and patch availability.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.007: JavaScript
Persistence	T1505: Server Software Component	T1505.003: Web Shell

Tactic	Technique	Sub-technique
Defense Evasion	T1070: Indicator Removal	T1070.002: Clear Linux or Mac System Logs
	T1620: Reflective Code Loading	
Credential Access	T1649: Steal or Forge Authentication Certificates	
	T1003: OS Credential Dumping	
Discovery	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1049: System Network Connections Discovery	
Collection	T1560: Archive Collected Data	T1560.001: Archive via Utility
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	T1090.002: External Proxy
	T1572: Protocol Tunneling	
	T1219: Remote Access Tools	T1219.002: Remote Desktop Software
Impact	T1486: Data Encrypted for Impact	
	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	d1caa376cb45b6a1eb3a45c5633c5ef75f7466b8601ed72c8022a8b3f6c1f3be, 6c8efbcef3af80a574cb2aa2224c145bb2e37c2f3d3f091571708288ceb22d5f
IPv4	206[.]251[.]239[.]164, 199[.]217[.]98[.]153, 89[.]46[.]237[.]33, 144[.]172[.]94[.]59, 199[.]217[.]99[.]121, 188[.]245[.]41[.]78, 144[.]172[.]110[.]106, 95[.]217[.]22[.]175, 37[.]27[.]244[.]222
Domains	cherryberry[.]click, ms-server-default[.]com, initialize-configs[.]com, ms-global.first-update-server[.]com, ms-sql-auth[.]com, kolonialeru[.]com, sclair.it[.]com, browser-updater[.]com, browser-updater[.]live, os-update-server[.]com, os-update-server[.]org, os-update-server[.]live, os-update-server[.]top
URL	hxxp[:]//ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid[.]onion/chat[.]php
Exploit TLS JA4	t13i1811h1_85036bcba153_b26ce05bbdd6, t13i4311h1_c7886603b240_b26ce05bbdd6
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
MD5	b885946e72ad51dca6c70abc2f773506, f80d3d09f61892c5846c854dd84ac403

Patch Links

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2

https://sec.cloudapps.cisco.com/security/center/softwarechecker.x

References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2

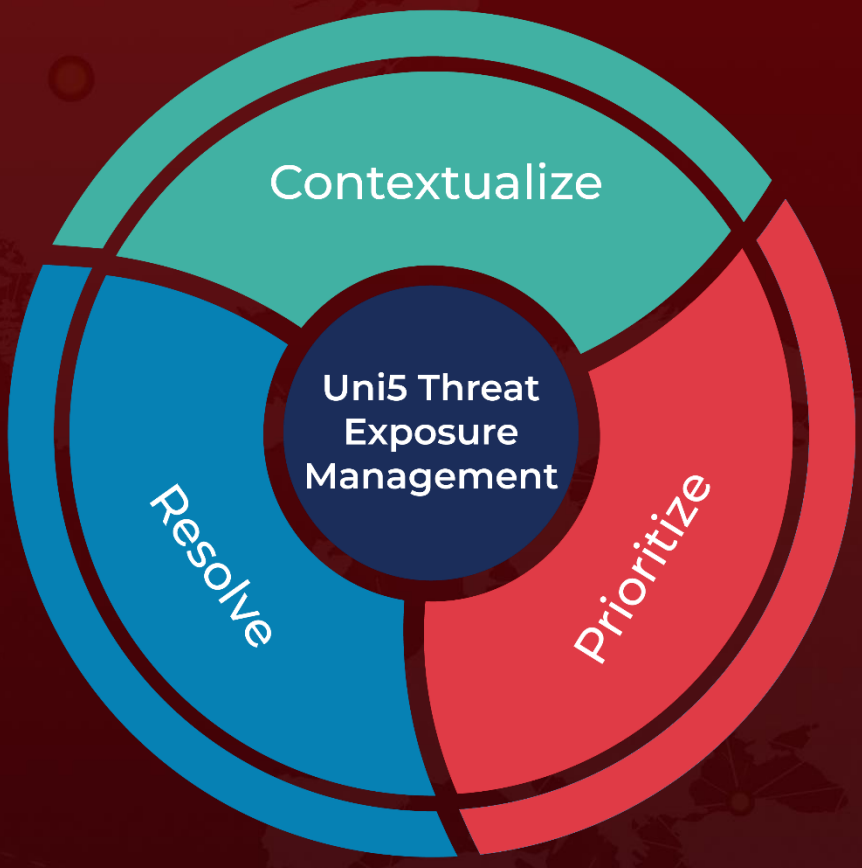
https://aws.amazon.com/blogs/security/amazon-threat-intelligence-teams-identify-interlock-ransomware-campaign-targeting-enterprise-firewalls/

https://hivepro.com/threat-advisory/interlock-ransomware-deploys-new-php-rat-via-filefix-phishing/

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

March 20, 2026 • 07:30 AM

More at www.hivepro.com