INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:32 UTC

Cisco Secure Firewall Management Center Dual CVSS 10 Vulnerabilities, Patch-Critical, No Workaround [SCC-2026-0008]

CVE VULNERABILITY | **CRITICAL** | CVSS 10.0

SCC Item ID	SCC-CVE-2026-0004
Type	CVE Vulnerability
CVE ID	CVE-2026-20079, CVE-2026-20131
Severity	CRITICAL
CVSS Base Score	10.0
Affected Products	Cisco Secure Firewall Management Center (FMC) Software — all on-premises releases. Cloud-Delivered FMC (cdFMC) not affected.
Published	20260306

Executive Summary

Cisco has released emergency patches for its Firewall Management Center, the administrative control platform used to manage Cisco firewall deployments across enterprise networks. Two separate vulnerabilities, both rated at the maximum possible severity, allow an attacker with no credentials and no access to execute commands as the highest-privilege user on the system. An attacker who compromises the Firewall Management Center gains effective control over every firewall it manages. No temporary workaround exists; patching is the only remedy. Organizations running Cisco FMC on-premises should treat this as a priority patching event this week.

Technical Analysis

Two maximum-severity (CVSS 10.0) vulnerabilities affect the web interface of Cisco Secure Firewall Management Center (FMC) on-premises deployments. CVE-2026-20079 is an authentication bypass (CWE-288) caused by an improperly initialized process created at boot time. An unauthenticated remote attacker can send crafted HTTP requests to exploit this process and execute scripts with root privileges on the underlying OS. The CVSS vector includes Scope:Changed (S:C), meaning successful FMC compromise also impacts managed Firewall Threat Defense (FTD) devices. CVE-2026-20131 is a Java deserialization vulnerability (CWE-502) in the same FMC web interface. An unauthenticated attacker can send a crafted serialized Java object to achieve RCE as root. All on-premises FMC software releases are affected. Cloud-Delivered FMC (cdFMC) is not affected and is patched by Cisco automatically. Neither critical

vulnerability is confirmed exploited in the wild as of 2026-03-06.

Action Checklist

1. DETECT, Identify all on-premises Cisco FMC instances in your environment. Cloud-Delivered FMC users require no action.n
2. CONTAIN, If immediate patching is not possible, restrict FMC web management interface access to trusted networks only via ACLs.n
3. MITIGATE, Apply Cisco fixed releases per advisory. Use Cisco Software Checker to identify the first fixed release for your current FMC version. No workarounds exist for CVE-2026-20079.n
4. VERIFY, Confirm patched FMC version string post-update and check normal authentication behavior.n
5. MONITOR, Monitor FMC access logs for unexpected HTTP requests; alert on any process spawning from the FMC web service that does not match a known baseline.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership and board risk committee immediately if any FMC instance cannot be patched within 24 hours, as an unauthenticated attacker can achieve complete control of all firewalls managed by that FMC with trivial exploit code; consider engaging external IR firm if internal team has not fully validated patch application or detected evidence of post-compromise activity in access logs.
Recovery Notes	Post-patching, monitor managed firewall policies and rules for unauthorized changes for 14 days; conduct a full forensic analysis of FMC logs (access, auth, audit, application) covering the past 30 days to detect any pre-patch compromise attempts or successful exploitation (look for non-standard HTTP methods, unusual auth failures followed by successes, or process spawns from Tomcat). If any evidence of exploitation is found, assume all firewalls managed by this FMC may be compromised and initiate firewall-level forensics (log analysis, traffic captures) and network-wide incident response.
Forensic Artifacts	/var/log/access.log (FMC web server access log — examine for non-standard HTTP methods, unusual URIs, 401/403/200 sequences suggesting auth bypass) | /var/log/auth.log (FMC system authentication log — look for privilege escalation, sudo attempts, or SSH login anomalies pre-patch) | /var/log/fmc.log and /var/log/fmc_startup.log (FMC application logs — check for startup errors, crashes, or suspicious debug output) | /var/log/audit.log (FMC audit log — document configuration changes, policy updates, user additions, or privilege changes) | Tomcat process tree and spawned child processes (run `pstree -p tomcat` and `ps aux | grep tomcat` to detect unauthorized command execution or reverse shells spawned from the FMC web service)

Per-Action IR Details

DETECT, Identify all on-premises Cisco FMC instances in your environment. Cloud-Delivered FMC users require no action.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: tools and resources)

Controls: NIST 800-53 CM-8 (Information System Component Inventory), CIS 6.1 (Establish and Maintain Detailed Asset Inventory)

Compensating: Query your asset management database or network scans for FMC hostnames (typically fmc.domain.local or fmc-prod). If no CMDB exists, use nmap: `nmap -p 443 -sV | grep -i cisco` or SSH to your firewall fleet and query managed device lists via CLI: `show managers` on ASA/Firepower. Document IP, hostname, version via SSH: `show version | include Model|Version`.

Evidence: Before patching, capture current FMC version string, build number, and management interface IP/hostname via SSH or web UI. Export the current device inventory managed by FMC (Administration > System > Managed Devices) as a baseline. Screenshot the web UI login page (shows build version) and save /var/log/fmc_startup.log from the FMC appliance to establish pre-patch state.

CONTAIN, If immediate patching is not possible, restrict FMC web management interface access to trusted networks only via ACLs.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2 (Containment: limiting scope and impact)

Controls: NIST 800-53 AC-3 (Access Control Enforcement), NIST 800-53 CA-7 (Continuous Monitoring), CIS 6.3 (Address Unauthorized Network Access)

Compensating: If FMC is behind a firewall you manage, add an inbound access control list (ACL) on the upstream firewall to permit TCP 443 (HTTPS) only from trusted admin IP ranges. On Linux FMC appliance directly: use `iptables` to restrict incoming traffic: `iptables -A INPUT -p tcp --dport 443 -s -j ACCEPT; iptables -A INPUT -p tcp --dport 443 -j DROP`. Persist with `iptables-save > /etc/iptables/rules.v4`. Document the ACL rules applied and the specific trusted networks whitelisted.

Evidence: Before applying ACLs, capture a full packet capture of FMC management traffic for 10 minutes using `tcpdump -i eth0 -w fmc_baseline.pcap -s 0 'tcp port 443'` to establish baseline management access patterns. Export current ACL rules from upstream firewalls. Document all legitimate admin IPs/ranges that must retain access. Capture FMC access logs for 24 hours prior: `/var/log/access.log` and `/var/log/fmc.log`.

MITIGATE, Apply Cisco fixed releases per advisory. Use Cisco Software Checker to identify the first fixed release for your current FMC version. No workarounds exist for CVE-2026-20079.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.3 (Eradication: removing the attack vector)

Controls: NIST 800-53 SI-2 (Flaw Remediation), NIST 800-53 CM-3 (Configuration Change Control), CIS 3.10 (Address Unauthorized Software)

Compensating: Organizations without Cisco support contracts can download patches from Cisco's Software Download Center (requires valid Cisco login). Identify your current FMC version via `show version` on the FMC CLI or web UI (Administration > System > Information). Cross-reference the version against Cisco's FMC release notes (https://www.cisco.com/c/en/us/support/security/secure-firewall-management-center/products-release-notes.html) to find the first patched release. Download the .iso or update bundle, verify SHA256 checksums against Cisco's published hashes before deployment. Test the patch in a lab environment or staging FMC instance first if possible; if not, schedule patching during a maintenance window with change control approval and rollback procedure documented.

Evidence: Capture the current running FMC version, build date, and all installed hotfixes: `show version` (full output). Export the complete system configuration as a backup before patching: use FMC web UI > System > Configuration > Backup & Restore or SSH: `backup system location `. Capture the pre-patch state of all managed devices (firewall inventory, policies, rules) via FMC API or export: `curl -X GET https://fmc.local/api/fmc_config/v1/domain//devicerecords -H 'X-auth-access-token: '`. Document all custom configurations, custom rules, or integrations running on FMC. Enable debug logging before patching: `/var/log/fmc.log` and `/var/log/fmc_startup.log` to capture patch installation logs.

VERIFY, Confirm patched FMC version string post-update and check normal authentication behavior.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Recovery: restoring to normal operations)

Controls: NIST 800-53 SI-7 (Information System Monitoring), NIST 800-53 IA-2 (User Authentication), CIS 6.2 (Address Unauthorized Access)

Compensating: Post-patch, SSH to FMC and confirm: `show version | include Build` — the build number must match or exceed Cisco's published fixed build for your version line. Test authentication by logging out and logging in via the web UI using a test admin account (not your primary account, to avoid lockout). Verify that all managed firewalls still appear in the device inventory (Administration > System > Managed Devices) and show 'Managed' status. Test one policy push to a managed firewall to confirm management plane functionality: deploy a test rule, then verify it appears on the firewall CLI. Check FMC process list: `ps aux | grep -i fmc` to ensure no unauthorized processes spawned during patching.

Evidence: After patching, capture the new version string: `show version` (full output, save to file for comparison against pre-patch baseline). Export the managed device list post-patch and compare against pre-patch baseline to detect any unauthorized devices. Capture FMC system logs during and after patching: `/var/log/fmc_startup.log`, `/var/log/fmc.log`, and `/var/log/audit.log` to verify normal boot and no suspicious startup activity. Test authentication logs: check for any failed login attempts or privilege escalations in `/var/log/auth.log` or via `show session` on FMC CLI. Take a fresh full system backup post-patch for recovery purposes.

MONITOR, Monitor FMC access logs for unexpected HTTP requests; alert on any process spawning from the FMC web service that does not match a known baseline.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 (Post-Incident Activities: monitoring to detect recurrence)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AU-2 (Audit Events), CIS 8.1 (Establish and Maintain Detailed Logging)

Compensating: Organizations without SIEM/EDR can monitor FMC logs locally using `tail -f /var/log/access.log | grep -v 'GET /api/fmc_config\|GET /api/fmc_platform\|GET /dashboard'` to surface anomalous HTTP requests (filter out known baseline requests). Create a baseline of legitimate process ancestry on FMC: run `ps -ef --forest | grep tomcat` or `pstree -p tomcat` to document normal child processes from the FMC web service (Tomcat). Monitor for deviations: `ps aux | grep -v grep | grep -v tomcat | awk '{print $NF}' > /tmp/baseline.txt` then daily run and diff against baseline to catch unauthorized spawns. Set up a daily cron job to parse `/var/log/access.log` and alert on HTTP 200 responses to non-standard paths: `grep -E '(POST|PUT|DELETE) /' /var/log/access.log | grep -v '/api/fmc' | mail -s 'FMC Anomaly' soc@company.com`. Review FMC audit logs weekly: `show audit` or tail `/var/log/audit.log` for privilege escalations, configuration changes, or user additions.

Evidence: Establish a post-patch baseline of normal FMC behavior: capture 48 hours of access logs (`/var/log/access.log`), auth logs (`/var/log/auth.log`), and FMC application logs (`/var/log/fmc.log`). Document the normal process tree spawned from Tomcat (the FMC web service): `pstree -p tomcat > /tmp/baseline_processes.txt`. Record the normal HTTP request patterns: `grep 'GET\|POST' /var/log/access.log | cut -d' ' -f7 | sort | uniq -c | sort -rn > /tmp/baseline_endpoints.txt`. Collect baseline network connections from FMC: `netstat -tuln | grep ESTABLISHED` to establish expected inbound/outbound connections. Set up log forwarding to a syslog server or local file with retention ≥90 days: `logger -n -P 514 < /var/log/fmc.log`. If EDR/SIEM is available, create detection rules for: (1) HTTP requests to FMC with status 200 and URI containing 'cmd' or 'exec' or 'bash'; (2) any process with parent=tomcat and child not in baseline_processes.txt; (3) any SSH/privilege escalation post-patch.

Detection Guidance

Monitor FMC web server access logs for abnormal HTTP request patterns to the management interface. Alert on any process execution spawned from the FMC web service process context, particularly shell execution or Java process creation. Look for Java serialization magic bytes (0xAC ED 00 05) in HTTP POST request bodies to the FMC management interface if SSL inspection is available. Establish a baseline of normal boot-time processes and alert on new or unexpected processes created at startup (relevant to CVE-2026-20079 boot-time process anomaly).

Indicators of Compromise

Type	Value	Context	Confidence
URL	`/api/fmc_config/v1/`	Cisco FMC REST API endpoint commonly targeted in authentication bypass and remote code execution attempts against the management interface	MEDIUM
URL	`/api/fmc_platform/v1/auth/generatetoken`	FMC REST API token generation endpoint that may be abused in authentication bypass scenarios related to critical FMC vulnerabilities	MEDIUM
FILE_PATH	`/var/sf/htdocs/`	Cisco FMC web application root directory; unexpected file creation here may indicate web shell deployment following exploitation	MEDIUM
FILE_PATH	`/var/sf/htdocs/*.jsp`	JSP web shell files placed in the FMC web root following successful exploitation; monitor for unexpected JSP file creation	MEDIUM
FILE_PATH	`/var/sf/htdocs/*.php`	PHP web shell files placed in the FMC web root following successful exploitation; monitor for unexpected PHP file creation	MEDIUM
FILE_PATH	`/ngfw/var/log/`	Cisco FMC system log directory; review for anomalous authentication events, privilege escalation, or unexpected process execution	MEDIUM
FILE_PATH	`/var/log/httpd/`	Apache HTTP server logs on FMC appliance; review for unusual HTTP request patterns, anomalous URIs, or high-frequency requests from single sources	HIGH

Type	Value	Context	Confidence
FILE_PATH	`/var/log/httpd/ssl_access_log`	This file is suspicious when accessed or modified by non-httpd processes or when containing HTTP requests with malformed headers, SQL injection payloads, or path traversal sequences targeting /admin or /api endpoints, as legitimate HTTPS access logs are written only by the Apache httpd daemon and should contain standard HTTP requests from expected management networks; deviation indicates potential exploitation of FMC authentication or session handling vulnerabilities.	HIGH
FILE_PATH	`/etc/cron.d/`	Cron directory on FMC appliance; threat actors may establish persistence by adding cron jobs after successful exploitation	MEDIUM
FILE_PATH	`/tmp/`	Suspicious when SYSTEM-privileged processes write executable files or scripts to /tmp/ spawned from web service processes (java.exe, tomcat), management interfaces (https listeners), or child processes of vulnerable applications without corresponding package manager activity or compilation artifacts; legitimate use involves orchestrated writes from apt/yum/installer processes with expected parent-child relationships and cleanup operations, whereas post-exploitation staging shows direct file writes followed by immediate execution from the same process tree with no cleanup, indicating payload staging rather than standard software installation.	MEDIUM
URL	`/ui/login`	FMC web UI login endpoint; monitor for brute force attempts, credential stuffing, or anomalous authentication patterns preceding exploitation	MEDIUM
URL	`/api/fmc_config/v1/domain/default/policy/`	FMC REST API policy management endpoint; unauthorized access may indicate post-exploitation policy manipulation to weaken firewall rules	MEDIUM

Type	Value	Context	Confidence
REGISTRY_KEY	`N/A - Linux-based appliance`	Cisco FMC runs on a Linux-based OS; registry keys are not applicable. Focus on file system, process, and network-based indicators	HIGH
FILE_PATH	`/usr/local/sf/bin/`	Cisco FMC binary directory; monitor for unexpected binaries or modifications to existing executables indicating post-exploitation tampering	MEDIUM
URL	`/api/fmc_config/v1/domain/default/devices/devicerecords`	FMC device records API endpoint; unauthorized enumeration of managed devices may occur during post-exploitation reconnaissance	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1059** — Command and Scripting Interpreter
- **T1068** — Exploitation for Privilege Escalation

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-6** — Least Privilege

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T1068	Exploitation for Privilege Escalation	Privilege-Escalation

Sources

Source	URL	Tier
Security Affairs, March 5, 2026	https://securityaffairs.com/188921/security/cisco-fixes-maximum-sev...	T3
Abstract Security	https://www.abstract.security/blog/critical-cisco-vulnerabilities-c...	T3
Hackread, March 6, 2026	https://hackread.com/cisco-patches-firewall-vulnerabilities-cvss-10...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20079, CVE-2026-20131	T1
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3

Generated 2026-03-29 18:32 UTC by TJS Security Command Center