INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:43 UTC

US officials issue ‘emergency’ cybersecurity order after hackers breach at least one government agency

THREAT CAMPAIGN | CRITICAL

SCC Item ID	SCC-CAM-2026-0007
Type	Threat Campaign
Severity	CRITICAL
Affected Products	Cisco networking equipment (specific product/version not confirmed in available sources)
Published	Sep 25, 2025

Executive Summary

CISA issued an emergency directive on September 25, 2025, after confirmed unauthorized access to at least one US federal agency involving Cisco networking infrastructure. Private sector analysts assess the threat actors as state-sponsored, though no official government attribution has been made. Federal agencies face immediate compliance obligations under the directive; organizations running Cisco networking equipment should treat this as an active threat requiring urgent attention until technical details are released.

Technical Analysis

CISA's emergency directive was triggered by confirmed unauthorized access to at least one federal agency network involving Cisco infrastructure. Specific affected products, firmware versions, and CVE identifiers have not been confirmed in available open sources as of this report. MITRE ATT&CK techniques associated with this incident profile include T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), and T1133 (External Remote Services), suggesting the attack chain may have involved exploitation of an internet-exposed Cisco device, credential abuse, or compromise of remote access services. No CVEs, CWEs, CVSS scores, or confirmed IOCs have been publicly disclosed. No CISA KEV entry is confirmed for a specific CVE tied to this incident. Monitor CISA's official emergency directives page and Cisco's PSIRT advisories for technical updates. Note: source quality for this item is moderate (0.64); all sources are Tier 3 media. Authoritative technical detail should be sourced directly from CISA's official directive when published.

Action Checklist

1. Step 1, Immediate: Locate and review the official CISA emergency directive at cisa.gov/emergency-directives for mandatory compliance actions and deadlines applicable to federal agencies; non-federal operators should treat guidance as best practice.
2. Step 2, Immediate: Audit all internet-exposed Cisco networking devices (routers, switches, firewalls, VPN concentrators) for unauthorized access, active sessions, and configuration changes made since September 20, 2025.
3. Step 3, Detection: Review authentication logs on Cisco devices for T1078 indicators, unexpected account usage, off-hours logins, logins from unusual source IPs, or new local accounts created without change tickets.
4. Step 4, Detection: Check for T1133 exposure, inventory all Cisco remote access services (AnyConnect, SSL VPN, SSH management interfaces) exposed to the internet and verify access controls and MFA enforcement.
5. Step 5, Assessment: Cross-reference your Cisco device inventory against Cisco PSIRT advisories (sec.cloudapps.cisco.com/security/center/publicationListing.x) for any recently published high or critical advisories that align with T1190 exploitation patterns.
6. Step 6, Communication: Brief leadership on the emergency directive, potential exposure, and compliance status; notify your SOC and network engineering teams to prioritize Cisco device monitoring until further guidance is issued.
7. Step 7, Long-term: Review network segmentation and management plane access controls for all Cisco infrastructure; ensure out-of-band management, disable unused remote access protocols, and enforce least-privilege account policies.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	If any Cisco device is found with unauthorized user accounts, configuration changes post-September 20, or active T1133/T1078 indicators, or if your organization is a federal agency, escalate immediately to your CISO, legal, and OMB — and to an external IR firm if you lack in-house forensic capability.
Recovery Notes	Post-containment: patch all vulnerable Cisco devices to versions meeting CISA guidance, reset all administrative credentials via out-of-band channel, force re-authentication of all remote access sessions, and conduct a 30-day forensic review of Cisco logs for indicator persistence. Implement continuous monitoring of Cisco authentication and VPN logs using rules that fire on T1078 and T1133 patterns; alert threshold: one anomaly triggers analyst review within 15 minutes.
Forensic Artifacts	Cisco device running-config and startup-config (with timestamps, hash verification) | Syslog entries (severity 0–5) spanning September 20, 2025, to present (focus: %AAA, %SEC, %CRYPTO, %SSH, %SNMP authentication keywords) | Command history and audit trail from AAA/TACACS+ backend (if centralized; otherwise local `show history` per device) | VPN session logs: user, source IP, timestamp, authentication method, session duration, bytes transferred (for AnyConnect, SSL VPN, IPSec) | Netflow or syslog-exported connection logs showing flows to/from internet-facing Cisco devices (focus: ports 22, 443, 500, 1194, 1723; unexpected source IPs)

Per-Action IR Details

Step 1, Immediate: Locate and review the official CISA emergency directive at cisa.gov/emergency-directives for mandatory compliance actions and deadlines applicable to federal agencies; non-federal operators should treat guidance as best practice.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: tools, policies, procedures)

Controls: NIST 800-53 IR-1 (Incident Response Policy), NIST 800-53 CA-2 (Security Assessments), CIS 17.1 (Maintain Incident Response Plan)

Compensating: If cisa.gov is inaccessible, retrieve the directive via Internet Archive (web.archive.org) or request it directly from CISA's public portal. Document the retrieval source and timestamp for audit trail. Store locally and brief all stakeholders within 2 hours of receipt.

Evidence: Capture the directive PDF with metadata (download timestamp, checksum), document your organizational review notes with dates/times, and preserve any internal communications referencing compliance deadlines or scope decisions for chain-of-custody.

Step 2, Immediate: Audit all internet-exposed Cisco networking devices (routers, switches, firewalls, VPN concentrators) for unauthorized access, active sessions, and configuration changes made since September 20, 2025.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis: examination of logs and data)

Controls: NIST 800-53 AU-2 (Audit Events), NIST 800-53 SI-4 (Information System Monitoring), CIS 8.2 (Collect and Analyze Logs), CIS 8.6 (Centralize Log Storage)

Compensating: For organizations without SIEM: use `show log | include SESSION` on Cisco IOS/IOS-XE devices; export running-config and compare against saved baseline configs from September 19 using diff tools (diff, Beyond Compare, or WinMerge). For firewalls: extract connection logs via CLI (`show conn` on ASA, `show session` on Meraki) and parse with grep/awk to identify sessions from September 20 onward. Document device firmware version and last config save timestamp.

Evidence: Preserve device running-config (before any modifications), syslog exports (all severity levels) from September 20 onward, command history (`show history` or syslog auth records), active session snapshots, and any configuration backup files with timestamps. Hash all files for integrity verification.

Step 3, Detection: Review authentication logs on Cisco devices for T1078 indicators, unexpected account usage, off-hours logins, logins from unusual source IPs, or new local accounts created without change tickets.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.3 (Log and data analysis), NIST 800-53 AU-6 (Audit Review, Analysis, and Reporting)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 IA-4 (Identifier Management), CIS 5.2 (Use MFA for All Logins), CIS 6.1 (Establish an Access Control Process)

Compensating: Extract syslog entries containing 'User' or 'login' keywords; search for lines with timestamps outside business hours (off-hours definition per your org policy, typically 18:00–06:00 weekdays + all weekends). Use grep + awk: `grep -i 'user.*login\|account created' syslog.txt | awk -F'|' '$2 > "18:00" || $2 < "06:00"'`. Cross-reference source IPs against your known management IP ranges; flag IPs outside that range. Manually verify each unexpected login against your change management system (ticket number, approver, date).

Evidence: Preserve all syslog entries with authentication keywords (AAA, login, user, account, privilege) from September 20 onward with full timestamps and source IP context. Extract local user database (`show run | include username`) and capture it with a timestamp. Save any audit trail or login history reports native to the device OS.

Step 4, Detection: Check for T1133 exposure, inventory all Cisco remote access services (AnyConnect, SSL VPN, SSH management interfaces) exposed to the internet and verify access controls and MFA enforcement.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (Vulnerability analysis), NIST 800-53 CA-7 (Continuous Monitoring)

Controls: NIST 800-53 AC-3 (Access Enforcement), NIST 800-53 IA-2 (Multi-Factor Authentication), CIS 5.2 (MFA for All Logins), CIS 13.2 (Detect and Alert on VPN Usage)

Compensating: Use nmap or Shodan API to enumerate internet-facing ports (443, 22, 500, 1194) on your public IP ranges; cross-reference results against your device inventory. On each Cisco device, run `show run | include aaa|mfa|tacacs|radius` to verify AAA methods are configured. For VPN concentrators: `show webvpn anyconnect sessions` and verify SAML/MFA in the AAA backend. Document MFA status (enabled/disabled) for each remote access method with timestamps. If MFA is absent, escalate immediately and enable as containment action.

Evidence: Preserve network scan results (IP, port, service banner), running-config excerpts showing AAA/authentication configuration, VPN session logs (user, IP, timestamp), and MFA policy documents. Capture proof of MFA enablement (screenshot of AAA config or policy document) dated post-September 25.

Step 5, Assessment: Cross-reference your Cisco device inventory against Cisco PSIRT advisories (sec.cloudapps.cisco.com/security/center/publicationListing.x) for any recently published high or critical advisories that align with T1190 exploitation patterns.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.5 (Vulnerability analysis and threat intelligence integration), NIST 800-53 SI-5 (Security Alerts, Advisories, and Directives)

Controls: NIST 800-53 CA-7 (Continuous Monitoring), NIST 800-53 SI-2 (Flaw Remediation), CIS 2.3 (Address Unauthorized Software), CIS 7.2 (Ensure Software Is Up to Date)

Compensating: Download the Cisco PSIRT RSS feed or JSON API (cisco.com/security); parse advisory titles for your device models and software versions. Use a spreadsheet (CSV): columns for Device Model, IOS Version, Applicable CVE, Severity, Publication Date. Filter for advisories published after September 15, 2025, and CVEs with CVSS ≥ 8.0. Cross-check each CVE against MITRE ATT&CK to identify T1190 (Exploit Public-Facing Application) indicators. Document which devices are vulnerable and their remediation status.

Evidence: Preserve Cisco PSIRT advisories (PDFs or HTML snapshots), your device inventory (model, serial, software version) with timestamps, a mapping document showing vulnerable devices, and proof of vulnerability scans (if available via free tools like OpenVAS or nessus community). Keep advisory retrieval timestamps for chain-of-custody.

Step 6, Communication: Brief leadership on the emergency directive, potential exposure, and compliance status; notify your SOC and network engineering teams to prioritize Cisco device monitoring until further guidance is issued.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.3.1 (Roles and responsibilities), NIST 800-53 IR-1 (Incident Response Policy)

Controls: NIST 800-53 IR-2 (Incident Response Training), NIST 800-53 CA-7 (Continuous Monitoring), CIS 17.1 (Maintain Incident Response Plan), CIS 17.2 (Establish Incident Response Contact List)

Compensating: Create a one-page summary: Threat Overview (campaign, Cisco focus, state-sponsored assessment), Your Exposure (device count, internet-exposed count, MFA status), Compliance Obligations (federal agency compliance vs. best practice for others), Detection Actions (specific log sources to monitor), Escalation Criteria (what triggers external IR), and Contact List (SOC lead, network admin, CISO, external IR firm). Distribute via secure email; schedule a 30-minute war room within 2 hours to align priorities.

Evidence: Document distribution (recipient list, timestamp, delivery method), attendee acknowledgment at briefing, and any decisions made (e.g., 'Enable MFA on VPN by EOD September 26'). Keep meeting notes with action items, owners, and due dates.

Step 7, Long-term: Review network segmentation and management plane access controls for all Cisco infrastructure; ensure out-of-band management, disable unused remote access protocols, and enforce least-privilege account policies.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Recovery phase: corrective actions), NIST 800-53 SC-7 (Boundary Protection), AC-6 (Least Privilege)

Controls: NIST 800-53 SC-7 (Boundary Protection), NIST 800-53 AC-6 (Least Privilege), NIST 800-53 AC-2 (Account Management), CIS 1.2 (Inventory and Control Hardware Assets), CIS 6.2 (Establish an Access Revocation Process)

Compensating: Implement using CLI commands: disable unneeded protocols (`no ssh`, `no http`, `no snmp` if not required); create dedicated management VLANs isolated from production traffic; restrict management access to a jump server or bastion host with logging enabled. Assign granular local roles (`privilege level 1–15`) and AAA groups to enforce separation of duties. Use `access-list` or `route-map` to restrict telnet/SSH to specific management IPs only. Document all changes in a network security baseline document with approval signatures.

Evidence: Preserve before/after running-configs (with timestamps and approver names), access control policy documents, network diagram showing management plane isolation, and logs of configuration changes (syslog excerpts showing admin actions). Maintain evidence for 12 months post-incident per NIST 800-61r3 §3.4.

Detection Guidance

No confirmed IOCs, CVEs, or specific attack signatures have been released in available open sources. Detection should focus on behavioral indicators aligned with the mapped ATT&CK techniques. For T1190 (Exploit Public-Facing Application): review Cisco device syslog and AAA logs for anomalous HTTP/HTTPS requests to management interfaces, unexpected process restarts, or configuration changes without corresponding change records. For T1078 (Valid Accounts): query authentication logs for accounts authenticating outside normal business hours, from unfamiliar source IPs, or to devices they do not normally access, particularly privileged or service accounts. For T1133 (External Remote Services): audit active VPN and remote management sessions; look for sessions with unusual duration, data transfer volumes, or originating from ASNs inconsistent with your user base. If your SIEM ingests Cisco syslog, build or enable detections for: failed login spikes followed by successful login on the same account, configuration archive commands run interactively, and privilege escalation events on IOS/NX-OS. Cross-reference any findings against known Cisco PSIRT bulletins active at time of incident. Monitor CISA's official directive for any IOC release.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`NOT AVAILABLE`	No IOCs confirmed in available open sources as of report date. Monitor CISA emergency directive publication for official IOC release.	LOW

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1078** — Valid Accounts
- **T1133** — External Remote Services

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
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1133	External Remote Services	Persistence

Sources

Source	URL	Tier
Cnn	https://www.cnn.com/2025/09/25/politics/hackers-breach-us-government	T3
US officials issue 'emergency' cybersecurity order after hackers ...	https://kesq.com/news/national-politics/cnn-us-politics/2025/09/25/...	T3
US issues 'emergency' cybersecurity order after hacker breach - KETV	https://www.ketv.com/article/us-officials-issue-emergency-cybersecu...	T3
US cyber officials issue 'emergency directive' after hackers breach ...	https://www.the-independent.com/news/world/americas/us-politics/eme...	T3

Source	URL	Tier
US cyber officials issued an “emergency directive” Thursday ...	https://www.threads.com/@cnn/post/DPDIFwLCibO/us-cyber-officials-is...	T3

Generated 2026-03-29 18:43 UTC by TJS Security Command Center