INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-17 18:52 UTC

Large-Scale Credential Harvesting Campaign Compromises 30,000+ Fortinet Devices Across 196 Countries

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0502
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Fortinet network infrastructure devices, unspecified product lines; likely includes FortiGate VPN/firewall endpoints and management interfaces based on campaign profile
Published	2026-06-17T10:06:34
Discovery Source	Rss

Executive Summary

A large-scale credential-harvesting campaign has compromised more than 30,000 Fortinet network devices across 196 countries, capturing working login credentials that attackers can use for unauthorized access, lateral movement, or ransomware deployment. Organizations running Fortinet VPN or firewall endpoints exposed to the internet are at elevated risk, particularly if credentials have not been rotated recently. CISA and the Canadian Centre for Cyber Security have both issued advisories confirming active exploitation of Fortinet authentication vulnerabilities in the same period, indicating the current urgency of this campaign.

Technical Analysis

This campaign targets Fortinet network infrastructure devices, likely FortiGate VPN and firewall endpoints, exploiting weaknesses in authentication mechanisms (CWE-287: Improper Authentication), insufficiently protected credentials (CWE-522), and potentially hardcoded or default credentials (CWE-798). MITRE techniques observed or likely in play include brute force and credential stuffing (T1110), exploitation of external remote services (T1133), exploitation of public-facing applications (T1190), credential harvesting from credential stores (T1555), valid accounts abuse (T1078), credential gathering via email/accounts (T1589.001), and modification of authentication processes (T1556). CISA issued guidance on 2026-01-28 addressing active exploitation of an authentication bypass vulnerability in Fortinet products (referenced as CVE-2026 series). CIS and CCCS advisories confirm multiple Fortinet vulnerabilities allowing arbitrary code execution are being

actively exploited. No specific CVE ID was confirmed in the source data for this campaign; attribution remains unknown. The geographic scope, 196 countries, indicates automated, opportunistic collection. Confidence: medium; campaign scope from Dark Reading (T3); CISA and CCCS advisories (T1/T3) corroborate active exploitation timeline.

Action Checklist

1. Step 1: Containment, Immediately restrict management interface access on all Fortinet devices to internal, trusted IP ranges only; disable internet-facing exposure of FortiGate administrative portals per CISA guidance (2026-01-28 advisory). Verify no management interfaces are publicly reachable. Apply NIST AC-17 (Remote Access) controls to enforce connection restrictions.
2. Step 2: Detection, Review Fortinet device authentication logs for anomalous login activity: repeated failed attempts (T1110), successful logins from unexpected geographic locations or IP ranges, and logins at unusual hours. Query logs for activity matching T1133 (External Remote Services) and T1078 (Valid Accounts). Cross-reference source IPs against known threat feeds. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs) to ensure logs are centralized and reviewed. Use D3-LAM (Local Account Monitoring) to flag anomalous local account activity.
3. Step 3: Eradication, Rotate all credentials on affected Fortinet devices immediately, including VPN user accounts, administrative accounts, and service accounts. Disable or rename default accounts per CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software). Apply all available Fortinet security patches addressing the CVE-2026 series authentication bypass vulnerabilities referenced in the CISA advisory. Consult the CCCS advisory AV26-059 and CIS advisory 2026-003 for specific patch guidance. Apply D3-CRO (Credential Rotation) and D3-CH (Credential Hardening).
4. Step 4: Recovery, After credential rotation and patching, verify that no unauthorized accounts or backdoors were created during the compromise window by reviewing account inventories against CIS 5.1 (Establish and Maintain an Inventory of Accounts). Confirm MFA is enforced on all Fortinet administrative and VPN access per CIS 6.3, 6.4, and 6.5, and apply D3-MFA (Multi-factor Authentication). Monitor for resumed adversary activity, particularly lateral movement attempts, using NIST SI-4 equivalent logging and AU-6 continuous review for a minimum of 30 days post-remediation.
5. Step 5: Post-Incident, Conduct a lessons-learned review against the control gaps this campaign exposed: insufficient management interface access controls (NIST AC-17, AC-6), absence of MFA on VPN and admin surfaces (CIS 6.3-6.5), and inadequate credential protection practices (CWE-522, CWE-798). Update your vulnerability management process per CIS 7.1 and 7.2 to include Fortinet device firmware in automated patch tracking. Document a remediation process for future Fortinet advisories with defined SLA timelines.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership and legal counsel immediately if FortiGate authentication logs confirm successful logins from attacker-controlled IPs during the compromise window, if any downstream internal systems show lateral movement indicators (new admin accounts, unexpected SMB connections, anomalous DNS queries from the FortiGate segment), or if the organization is subject to HIPAA, PCI-DSS, or state breach notification laws and PII/PHI was accessible through the compromised VPN tunnel.
Recovery Notes	After patching and credential rotation, run a full account audit on internal systems reachable via the compromised FortiGate VPN tunnel — not just the Fortinet devices themselves — since harvested VPN credentials may have enabled lateral movement before detection. Implement continuous authentication log forwarding from all FortiGate devices to a centralized syslog server for a minimum of 30 days, specifically monitoring for `type=event subtype=vpn action=tunnel-up` events originating from IPs that were flagged during the detection phase. Do not declare recovery complete until MFA is enforced on all administrative and VPN access surfaces and the account inventory has been fully reconciled against the pre-compromise baseline.
Forensic Artifacts	FortiGate event logs (`type=event subtype=vpn` and `type=event subtype=admin`) stored on-disk at /var/log/log/ or exportable via `execute log filter; execute log display` — these record credential-use events including source IP, username, timestamp, and tunnel establishment status specific to this credential-harvesting campaign's replay activity. | FortiGate session table snapshot (`diagnose sys session list`) captured before any containment action — records active TCP/UDP sessions that may represent attacker-held VPN tunnels established using harvested credentials, including remote IP and session duration. | FortiGate running configuration export (`show full-configuration`) — preserves the complete admin and VPN user account list at time of compromise, enabling post-eradication diffing to identify backdoor accounts created by the attacker during their access window. | Network flow data (NetFlow/IPFIX) or firewall traffic logs from the segment behind the FortiGate VPN termination point — specifically flows initiated from VPN-assigned IP pools to internal servers, which would reveal lateral movement activity conducted using the harvested credentials after successful VPN authentication. | Syslog or RADIUS/LDAP authentication server logs for the identity backend used by FortiGate VPN (if external auth is configured) — records successful and failed authentication attempts passed through from the FortiGate, providing a corroborating source independent of the potentially compromised device's own logs.

Per-Action IR Details

Step 1: Containment — Immediately restrict management interface access on all Fortinet devices to internal, trusted IP ranges only; disable internet-facing exposure of FortiGate administrative portals per CISA guidance (2026-01-28 advisory). Verify no management interfaces are publicly reachable. Apply NIST AC-17 (Remote Access) controls to enforce connection restrictions.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-17 (Remote Access), NIST AC-3 (Access Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run `curl -sk https:///login` from an external IP to confirm the management portal is no longer reachable. Use iptables or Windows Firewall rules on any jump host to whitelist only trusted RFC 1918 ranges. Enumerate exposed FortiGate management IPs with `nmap -p 443,8443,10443 --open ` from an external vantage point before and after restriction to confirm closure.

Evidence: Before modifying any ACL or firewall rule that will terminate active management sessions: export the full FortiGate session table via `diagnose sys session list` (SSH/CLI) and capture `diagnose debug flow` output to record

all active management-plane connections. Preserve the running configuration snapshot (`show full-configuration`) and note any source IPs currently holding authenticated management sessions — these may be attacker-controlled pivot points that disappear once the interface is locked down.

Step 2: Detection — Review Fortinet device authentication logs for anomalous login activity: repeated failed attempts (T1110), successful logins from unexpected geographic locations or IP ranges, and logins at unusual hours. Query logs for activity matching T1133 (External Remote Services) and T1078 (Valid Accounts). Cross-reference source IPs against known threat feeds. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs) to ensure logs are centralized and reviewed. Use D3-LAM (Local Account Monitoring) to flag anomalous local account activity.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, SSH to each FortiGate and run `log filter field user ` combined with `execute log filter device disk` and `execute log display` to pull authentication events locally. Export logs via `execute backup log tftp ` and parse offline with `grep` for `action=login` and `status=failed` or `status=success` paired with unexpected `srcip` values. Cross-reference source IPs against Abuse IPDB or CISA's known-bad IP lists using a simple bash loop with `curl https://api.abuseipdb.com/api/v2/check?ipAddress=`.

Evidence: This campaign harvests and replays working credentials, so the highest-value volatile artifact is the FortiGate authentication event log stored in RAM-backed syslog buffers before log rotation: capture `get log memory filter` and `execute log filter device memory; execute log display` immediately. Also record the output of `get system session list` and `diagnose vpn tunnel list` to identify active VPN sessions established with harvested credentials — these sessions vanish on device reload or credential rotation.

Step 3: Eradication — Rotate all credentials on affected Fortinet devices immediately, including VPN user accounts, administrative accounts, and service accounts. Disable or rename default accounts per CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software). Apply all available Fortinet security patches addressing the CVE-2026 series authentication bypass vulnerabilities referenced in the CISA advisory. Consult the CCCS advisory AV26-059 and CIS advisory 2026-003 for specific patch guidance. Apply D3-CRO (Credential Rotation) and D3-CH (Credential Hardening).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 5.2 (Use Unique Passwords), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Enumerate all local FortiGate admin accounts via `config system admin; show` (CLI) and all VPN user accounts via `config user local; show` before rotation — screenshot or export to a text file as the pre-rotation baseline. For credential rotation without a PAM tool, use a password manager (Bitwarden free tier) to generate unique 20+ character passwords per account. Apply firmware updates via the FortiGate web GUI under System > Firmware, verifying the downloaded image hash against Fortinet's published SHA256 on support.fortinet.com before upload.

Evidence: Credential rotation and patching alter live authentication state and may overwrite indicators of attacker-created accounts. Before rotating or patching: export `config system admin; show` and `config user local; show` in full to capture any backdoor accounts the attacker may have created during the compromise window. Run `diagnose sys session list | grep 'proto=6'` to record all active TCP sessions that may represent persistent attacker connections. Capture `get hardware nic ` ARP tables to record any lateral movement pivot IPs. These artifacts are unrecoverable after a firmware update that clears volatile state.

Step 4: Recovery — After credential rotation and patching, verify that no unauthorized accounts or backdoors were created during the compromise window by reviewing account inventories against CIS 5.1 (Establish and

Maintain an Inventory of Accounts). Confirm MFA is enforced on all Fortinet administrative and VPN access per CIS 6.3, 6.4, and 6.5, and apply D3-MFA (Multi-factor Authentication). Monitor for resumed adversary activity — particularly lateral movement attempts — using NIST SI-4 equivalent logging and AU-6 continuous review for a minimum of 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Diff the pre-rotation admin account export (captured in Step 3 evidence) against a fresh `config system admin; show` output to surface any accounts added during the attacker's access window. Enable FortiGate's built-in two-factor authentication for admin accounts under System > Administrators using FortiToken Mobile (free for up to 2 tokens on FortiGate). Set up a daily cron job that SSH-exports `get log memory filter` output and emails it to the security team for manual review during the 30-day watch period.

Evidence: Recovery steps do not inherently destroy volatile evidence if eradication was completed first; however, before enabling MFA enforcement (which may terminate active sessions), run a final `diagnose sys session list` and `diagnose vpn tunnel list` to confirm no attacker-held sessions survived credential rotation. If any suspicious session is found, treat this as an active re-compromise and revert to containment phase before proceeding with recovery.

Step 5: Post-Incident — Conduct a lessons-learned review against the control gaps this campaign exposed: insufficient management interface access controls (NIST AC-17, AC-6), absence of MFA on VPN and admin surfaces (CIS 6.3–6.5), and inadequate credential protection practices (CWE-522, CWE-798). Update your vulnerability management process per CIS 7.1 and 7.2 to include Fortinet device firmware in automated patch tracking. Document a remediation process for future Fortinet advisories with defined SLA timelines.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-17 (Remote Access), NIST AC-6 (Least Privilege), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Schedule a structured 60-minute lessons-learned meeting within 5 business days of recovery closure; use the NIST 800-61r3 §4 questions as the agenda template (what happened, how was it detected, what was the impact, what worked, what did not). Add FortiGate firmware to a monthly patch-check checklist using Fortinet's PSIRT RSS feed (https://www.fortiguard.com/rss/ir.xml — verify URL resolves before using) so future advisories are caught within 24 hours of publication rather than after mass-compromise notifications.

Evidence: No volatile evidence capture is required at this phase — all live state should have been preserved during earlier phases. The primary inputs for the lessons-learned review are: the pre/post account inventory diff from Step 3, the authentication log exports from Step 2, the timeline of attacker access reconstructed from FortiGate event logs (`type=event subtype=vpn` and `type=event subtype=admin`), and the original CISA 2026-01-28 advisory and CCCS AV26-059 to confirm whether the organization met the recommended remediation SLA.

Detection Guidance

Query Fortinet device authentication logs and any centralized SIEM for the following indicators: (1) High-volume failed login attempts against FortiGate management interfaces or SSL-VPN portals from single or rotating IPs, consistent with T1110 (Brute Force/Credential Stuffing). (2) Successful authentications from IP addresses or countries not matching organizational baselines, consistent with T1078 (Valid Accounts) abuse post-harvest. (3) Authentication events outside business hours for administrative accounts. (4) Any use of default or factory

credential pairs (admin/admin, admin/password), CWE-798 indicator. (5) Configuration changes or new account creation following successful authentication, potential persistence activity. Log sources: FortiGate event logs (auth category), SSL-VPN logs, system event logs. Aggregate via AU-6 (Audit Record Review) processes. Apply D3-LAM (Local Account Monitoring) for ongoing account anomaly detection and D3-UAP (User Account Permissions) review to identify privilege changes. No confirmed IOCs (IPs, domains, hashes) were available in the source data for this campaign; detection relies on behavioral and authentication anomaly patterns.

Framework Mappings

MITRE-ATTACK

- **T1110** — Brute Force
- **T1133** — External Remote Services
- **T1190** — Exploit Public-Facing Application
- **T1556** — Modify Authentication Process
- **T1589.001** — Credentials
- **T1078** — Valid Accounts
- **T1555** — Credentials from Password Stores

NIST-800-53R5

- **AC-7** — Unsuccessful Logon Attempts
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **SC-7** — Boundary Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **CP-9** — System Backup
- **IR-4** — Incident Handling
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A04:2021** — Insecure Design

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **5.2** — Use Unique Passwords
- **16.10** — Apply Secure Design Principles in Application Architectures

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1110	Brute Force	Credential-Access
T1133	External Remote Services	Persistence
T1190	Exploit Public-Facing Application	Initial-Access
T1556	Modify Authentication Process	Credential-Access
T1589.001	Credentials	Reconnaissance
T1078	Valid Accounts	Defense-Evasion
T1555	Credentials from Password Stores	Credential-Access

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/sweeping-cre...	T3
Multiple Vulnerabilities in Fortinet Products Could Allow for Arbitrary ...	https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-for...	T3
Fortinet vulnerabilities: How to find affected assets - runZero	https://www.runzero.com/blog/fortinet-assets/	T3
Fortinet Releases Guidance to Address Ongoing Exploitation ... - CISA	https://www.cisa.gov/news-events/alerts/2026/01/28/fortinet-release...	T1
Fortinet security advisory (AV26-059) – Update 1	https://www.cyber.gc.ca/en/alerts-advisories/cyber-fortinet-securit...	T3

Generated 2026-06-17 18:52 UTC by TJS Security Command Center