INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-19 18:57 UTC

FortiBleed: Mass Credential Compromise Campaign Targeting 86,644 FortiGate Devices Across 194 Countries

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0521
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Fortinet FortiGate firewalls and VPN gateways running FortiOS prior to 7.2.11, 7.4.8, and 7.6.1
Published	2026-06-19T10:00:21
Discovery Source	Rss

Executive Summary

A Russian-speaking threat actor has reportedly harvested working credentials for over 86,000 internet-facing Fortinet FortiGate firewalls and VPN gateways across 194 countries, in a campaign combining credential stuffing with passive traffic sniffing. Organizations running unpatched FortiOS versions face active credential compromise on their network perimeter devices, with telecom, government, and education sectors showing the highest exposure. Immediate action is required: upgrade to FortiOS 7.2.11, 7.4.8, or 7.6.1 and rotate all FortiGate credentials. Note: campaign-specific figures (device count, country spread, actor attribution) derive from a single news outlet and have not been independently corroborated by a CISA advisory or Fortinet bulletin in the available source set; treat as medium-confidence pending official confirmation.

Technical Analysis

The FortiBleed campaign targets Fortinet FortiGate firewalls and VPN gateways running FortiOS versions prior to 7.2.11, 7.4.8, and 7.6.1. No single CVE is assigned; the operation exploits four structural weaknesses: CWE-916 (use of legacy SHA-256 password hashing insufficient for modern credential protection), CWE-521 and CWE-255 (failure to enforce strong credentials and rotate defaults), and CWE-307 (absence of adequate brute-force protections enabling credential stuffing). The attack chain combines credential stuffing (T1110.001, T1110.003, T1110.004) with passive network sniffing (T1040) to harvest credentials from live traffic, then uses those credentials for valid account access (T1078, T1078.001) via external remote services (T1133). Account

manipulation (T1098) and credential gathering (T1589.001) sustain persistence. The self-reinforcing cycle - sniff credentials, stuff credentials, capture more credentials - allows durable access without requiring active exploitation of a patched vulnerability. Remediation targets are FortiOS 7.2.11, 7.4.8, and 7.6.1. Source quality score is 0.64; all campaign-scope figures are single-source.

Action Checklist

1. Step 1: Containment. Identify all internet-facing FortiGate firewalls and VPN gateways in your environment. Cross-reference running FortiOS versions against the affected range (any version prior to 7.2.11, 7.4.8, or 7.6.1). Restrict management-plane access (HTTPS, SSH) to trusted IP ranges immediately; disable public-facing admin interfaces where operationally feasible. Reference Fortinet Document Library release notes for 7.4.8 and 7.2.11 (see sources section) to confirm version targeting (CIS 1.1: maintain detailed asset inventory).
2. Step 2: Detection. Review FortiGate authentication logs for anomalous login activity: repeated failed attempts (indicative of T1110.001/T1110.003/T1110.004), successful logins from unexpected source IPs or geographies, and login events outside business hours. Enable logging of administrative authentication events and VPN session establishment if not already active (NIST AU-2: event logging; NIST AU-6: audit record review and analysis; CIS 8.2: collect audit logs). Query for concurrent or geographically implausible sessions on the same account (T1078). Inspect traffic logs for passive capture indicators, unusual outbound flows on management interfaces.
3. Step 3: Eradication. Upgrade all affected FortiGate devices to FortiOS 7.2.11, 7.4.8, or 7.6.1 per the Fortinet Document Library release notes. Follow the Fortinet upgrade path documentation to avoid skipping required intermediate versions. Immediately rotate all local FortiGate administrator credentials and VPN user credentials post-upgrade; enforce minimum password complexity requirements to address CWE-521 and CWE-255. Disable or rename default accounts where possible (CIS 4.7: manage default accounts; NIST AC-2: account management; D3-CRO: credential rotation; D3-CH: credential hardening).
4. Step 4: Recovery. After upgrading, validate the installed FortiOS version via the device CLI or management console. Confirm that brute-force lockout policies are active and configured (account lockout thresholds aligned to NIST AC-7: unsuccessful logon attempts). Re-audit administrator and VPN account inventories to remove orphaned or excessive accounts (NIST AC-6: least privilege; CIS 5.1: account inventory; CIS 5.3: disable dormant accounts). Monitor authentication logs for recurrence of anomalous patterns for a minimum of 30 days post-remediation (NIST AU-6).
5. Step 5: Post-Incident. Conduct a lessons-learned review against the four root-cause CWEs. Formalize a patch cadence policy ensuring perimeter device firmware is reviewed within 72 hours of a critical advisory (CIS 7.1: vulnerability management process; CIS 7.3: automated OS patch management). Implement MFA on all FortiGate administrative interfaces and VPN gateways (CIS 6.3, CIS 6.4, CIS 6.5: require MFA for external, remote, and administrative access; D3-MFA: multi-factor authentication). Enforce account lockout thresholds to block future credential stuffing (NIST AC-7). Review and formalize a credential rotation schedule for all network perimeter devices (D3-CRO).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO, legal counsel, and external IR retainer immediately if forensic review of FortiGate admin account list reveals unauthorized accounts or modified trusted-host entries (indicating post-compromise persistence), if VPN session logs confirm successful authentication from threat-actor-attributed IPs during the exposure window, or if the affected FortiGate devices terminate VPN sessions for regulated environments handling PII, PHI, or PCI-DSS cardholder data — all three conditions trigger breach notification assessment obligations.
Recovery Notes	After upgrading to FortiOS 7.2.11, 7.4.8, or 7.6.1 and rotating all administrator and VPN credentials, validate that no unauthorized admin accounts or trusted-host modifications were introduced by the threat actor by diffing the post-upgrade `show system admin` output against your pre-incident configuration baseline. Monitor FortiGate authentication logs (event category 1, subtype admin and VPN) daily for a minimum of 30 days for re-authentication attempts using the rotated account names from threat-actor-attributed IP ranges, as harvested credential lists from this campaign may be redistributed to secondary actors after the initial operator's use. If your FortiGate devices authenticate VPN users against Active Directory or LDAP, treat the directory as potentially exposed and audit for unauthorized AD accounts, password resets, or group membership changes originating from the FortiGate service account during the campaign window.
Forensic Artifacts	FortiGate event log (category 1, subtypes: admin, vpn) — will contain the credential-stuffing authentication failure bursts (high-volume failed logins against admin and VPN accounts) and successful logins immediately following, sourced from Russian-affiliated ASNs or anonymization infrastructure; export via `execute backup alllogs` before any log rotation. | FortiGate system admin configuration (`show system admin`) — preserves evidence of any unauthorized administrator accounts created for persistence, or modifications to `set trusthost` entries that would grant the threat actor persistent management-plane access after initial credential compromise. | SSL-VPN session monitor output (`get vpn ssl monitor` and `diagnose vpn ssl list`) — captures in-progress threat-actor VPN sessions with source IP, authenticated username, session duration, and bytes transferred; must be captured before session revocation or device isolation. | FortiGate traffic log (category 0) for management interface — may contain passive sniffing indicators: unexpected outbound connections from the FortiGate management interface to external IPs, or anomalous protocol activity on TCP/443 and TCP/22 consistent with credential exfiltration relay activity described in the campaign. | Running configuration backup (`show full-configuration` to file, timestamped pre-patch) — preserves the full device state at time of confirmed or suspected compromise, including routing tables, policy objects, and authentication server references that may reveal lateral movement staging or data exfiltration paths enabled by the threat actor using harvested credentials.

Per-Action IR Details

Step 1: Containment — Identify all internet-facing FortiGate firewalls and VPN gateways in your environment. Cross-reference running FortiOS versions against the affected range (any version prior to 7.2.11, 7.4.8, or 7.6.1). Restrict management-plane access (HTTPS, SSH) to trusted IP ranges immediately; disable public-facing admin interfaces where operationally feasible. Reference Fortinet Document Library release notes for 7.4.8 and 7.2.11 to confirm version targeting (CIS 1.1: maintain detailed asset inventory).

NIST Phase: Containment

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run `get system status` via SSH on each FortiGate to extract FortiOS version; pipe output to a text file for inventory. Use `shodan` CLI (free tier) or Censys to identify your own internet-exposed FortiGate management interfaces (filter: `product:FortiGate`). Apply a FortiOS firewall policy or router ACL upstream to block external access to TCP/443 and TCP/22 on the FortiGate management interface immediately, without waiting for console access to each device.

Evidence: Before restricting management-plane access, capture: current active administrative sessions (`get system session list` filtered for management ports TCP/443 and TCP/22), FortiGate running config (`show full-configuration`), and the current trusted host list for all admin accounts (`show system admin`). These will establish the pre-containment access baseline and may reveal unauthorized trusted-host additions that persist after credential rotation.

Step 2: Detection — Review FortiGate authentication logs for anomalous login activity: repeated failed attempts (indicative of T1110.001/T1110.003/T1110.004), successful logins from unexpected source IPs or geographies, and login events outside business hours. Enable logging of administrative authentication events and VPN session establishment if not already active (NIST AU-2: event logging; NIST AU-6: audit record review and analysis; CIS 8.2: collect audit logs). Query for concurrent or geographically implausible sessions on the same account (T1078). Inspect traffic logs for passive capture indicators, unusual outbound flows on management interfaces.

NIST Phase: Detection Analysis

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

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

Compensating: On FortiGate CLI, execute `execute log filter category 1` then `execute log display` to dump authentication event logs; export via syslog to a local rsyslog or Graylog instance (free). Parse for event subtypes `login` and `logout` with source IPs using grep: `grep -E '(action=login|action=logout)' fortigate_event.log | awk '{print $5,$9,$10}'`. For VPN session anomalies, query the SSL-VPN log: `execute log filter category 12` then `execute log display`. Flag any source IP not in your known-good list, any authentication event between 00:00–05:00 local time, or any account with more than one concurrent active session.

Evidence: This is a read-only analysis step that does not alter live state; however, capture the following volatile artifacts BEFORE proceeding to containment actions: (1) FortiGate memory-resident session table (`diagnose sys session list`) to capture active VPN and management sessions in progress; (2) active SSL-VPN tunnel table (`get vpn ssl monitor`) showing currently authenticated VPN users with source IPs and session durations; (3) raw FortiOS event log export from the device's local disk before any log rotation occurs (`execute backup alllogs ftp `). The credential-stuffing component of this campaign would leave high-volume failed-auth entries in event log category 1 (subtype: vpn or admin), and successful logins from Russian-affiliated ASNs or anonymization infrastructure (Tor exit nodes, residential proxies) immediately preceding or following failed bursts.

Step 3: Eradication — Upgrade all affected FortiGate devices to FortiOS 7.2.11, 7.4.8, or 7.6.1 per the Fortinet Document Library release notes. Follow the Fortinet upgrade path documentation to avoid skipping required intermediate versions. Immediately rotate all local FortiGate administrator credentials and VPN user credentials post-upgrade; enforce minimum password complexity requirements to address CWE-521 and CWE-255. Disable or rename default accounts where possible (CIS 4.7: manage default accounts; NIST AC-2: account management; D3-CRO: credential rotation; D3-CH: credential hardening).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

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

Compensating: Before patching, export running config (`execute backup config ftp `) and capture volatile state per the evidence field below. Use Fortinet's documented upgrade path tool at docs.fortinet.com to confirm required intermediate hops (e.g., 7.0.x → 7.2.x before 7.2.11). Post-upgrade, reset all admin account passwords via CLI (`config

system admin / edit / set password / end`) and bulk-reset LDAP-sourced VPN users at the directory level if LDAP authentication is in use. Use a password manager or a simple bash script with `openssl rand -base64 24` to generate unique credentials per account.

Evidence: Patching and credential rotation alter live state on a device that may hold evidence of active compromise. Capture BEFORE upgrading: (1) full running configuration (`show full-configuration` to file) to preserve any unauthorized admin accounts or trusted-host modifications inserted by the threat actor; (2) current admin account list with trusted hosts and last-login timestamps (`show system admin`); (3) FortiOS event log full export (category 0 and 1) for authentication and system events; (4) active VPN session table (`get vpn ssl monitor`) and IPsec tunnel status (`diagnose vpn tunnel list`) to document any active threat-actor sessions; (5) firmware version string (`get system status`) as a timestamped pre-patch baseline. If the device shows signs of active compromise (unauthorized admin accounts, unexpected trusted hosts, or active sessions from unknown IPs), treat the device as potentially implanted and escalate to forensic imaging of flash storage before patching.

Step 4: Recovery — After upgrading, validate the installed FortiOS version via the device CLI or management console. Confirm that brute-force lockout policies are active and configured (account lockout thresholds aligned to NIST AC-7: unsuccessful logon attempts). Re-audit administrator and VPN account inventories to remove orphaned or excessive accounts (NIST AC-6: least privilege; CIS 5.1: account inventory; CIS 5.3: disable dormant accounts). Monitor authentication logs for recurrence of anomalous patterns for a minimum of 30 days post-remediation (NIST AU-6).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-7 (Unsuccessful Logon Attempts), NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Validate FortiOS version post-upgrade with `get system status | grep Version`. Verify lockout policy via CLI: `show system global | grep -E '(admin-lockout-threshold|admin-lockout-duration)'`; set threshold to 5 attempts and duration to 300 seconds minimum if not already enforced. Audit all admin accounts with `show system admin` and flag any account without a `set trusthost` restriction or with last-login timestamps predating the campaign window. For VPN user audit, export `show user local` and cross-reference against HR active-employee list. Forward FortiGate syslog to a local Graylog or rsyslog instance and create a cron-driven daily alert (grep for `action=login` from non-whitelisted IPs) for the 30-day monitoring window.

Evidence: This step validates system integrity post-eradication and does not alter incident evidence; however, before re-enabling full management-plane access or restoring VPN services, verify: (1) no unauthorized admin accounts remain (`show system admin` count matches pre-incident baseline); (2) no unauthorized trusted-host entries exist on surviving admin accounts; (3) FortiOS upgrade completed without rollback (confirm running version matches target); (4) authentication log continuity — confirm syslog forwarding is active and no log gap exists between eradication and recovery phases, as a gap could conceal post-patch threat-actor re-entry attempts using harvested credentials that were not yet rotated.

Step 5: Post-Incident — Conduct a lessons-learned review against the four root-cause CWEs. Formalize a patch cadence policy ensuring perimeter device firmware is reviewed within 72 hours of a critical advisory (CIS 7.1: vulnerability management process; CIS 7.3: automated OS patch management). Implement MFA on all FortiGate administrative interfaces and VPN gateways (CIS 6.3, CIS 6.4, CIS 6.5: require MFA for external, remote, and administrative access; D3-MFA: multi-factor authentication). Enforce account lockout thresholds to block future credential stuffing (NIST AC-7). Review and formalize a credential rotation schedule for all network perimeter devices (D3-CRO).

NIST Phase: Post Incident

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

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.3 (Perform Automated Operating System Patch Management), 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), NIST AC-7 (Unsuccessful Logon Attempts), NIST AU-11 (Audit Record Retention)

Compensating: Enable FortiToken Mobile (free for up to 10 tokens on FortiAuthenticator free-tier) or integrate FortiGate with a RADIUS server backed by Google Authenticator (FreeRADIUS + libpam-google-authenticator, no cost) for MFA on admin logins and SSL-VPN. Document the lessons-learned review using the NIST 800-61r3 §4 template covering: timeline of FortiOS exposure window, scope of accounts confirmed or suspected compromised, detection gap analysis (how long were harvested credentials valid before discovery), and control gaps that allowed unpatched internet-facing FortiOS versions to persist. Subscribe to Fortinet PSIRT RSS feed (https://www.fortiguard.com/psirt) and create a calendar-triggered 72-hour review task for CRITICAL-rated FortiOS advisories.

Evidence: No live-state alteration occurs in this phase; retain and archive the following for the post-incident record and any downstream regulatory notification assessment: (1) full FortiGate event log exports (pre- and post-containment) covering the exposure window; (2) timestamped screenshots or CLI output of unauthorized account or trusted-host findings discovered during Step 3 audit; (3) VPN session records showing source IPs of sessions authenticated during the campaign window, for potential victim notification if third-party credentials were relayed; (4) the pre-patch running configuration backup as evidence of the device state at time of compromise. Retain all artifacts for a minimum period consistent with your jurisdiction's breach notification and records retention obligations.

Detection Guidance

Query FortiGate authentication logs for: (1) high-frequency failed login attempts against admin or VPN accounts within short time windows, consistent with credential stuffing (T1110.001, T1110.003, T1110.004); (2) successful authentications from IP addresses not in your expected administrative or user ranges; (3) VPN session establishments from geographies inconsistent with your user population (T1133, T1078); (4) multiple concurrent sessions for the same user account from different source IPs (T1078.001). On the network side, look for unexpected outbound traffic from FortiGate management interfaces that could indicate passive sniffing exfiltration (T1040). NIST AU-6 requires periodic review and analysis of audit records for anomalies; CIS 8.2 requires audit log collection to be enabled across the enterprise. If your SIEM is ingesting FortiGate syslog, build detection rules alerting on: login failure counts exceeding your defined threshold per account per hour, successful logins immediately following a burst of failures on the same account, and admin-plane access from public IP space. No specific IOCs (IPs, domains, hashes) have been confirmed in the available source set; behavioral detection is the primary available method at this time.

Framework Mappings

MITRE-ATTACK

- **T1098** — Account Manipulation
- **T1133** — External Remote Services
- **T1110.001** — Password Guessing
- **T1040** — Network Sniffing
- **T1110.004** — Credential Stuffing
- **T1589.001** — Credentials
- **T1110.003** — Password Spraying
- **T1078** — Valid Accounts
- **T1078.001** — Default Accounts

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **AC-7** — Unsuccessful Logon Attempts

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1098	Account Manipulation	Persistence
T1133	External Remote Services	Persistence
T1110.001	Password Guessing	Credential-Access
T1040	Network Sniffing	Credential-Access
T1110.004	Credential Stuffing	Credential-Access
T1589.001	Credentials	Reconnaissance
T1110.003	Password Spraying	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1078.001	Default Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/cisa-warns-fortinet-customers-as....	T3
Known issues | FortiGate / FortiOS 7.4.8 - Fortinet Document Library	https://docs.fortinet.com/document/fortigate/7.4.8/fortios-release-...	T3
Recommendation for Fortinet Devices - NetWorks Group	https://www.networksgroup.com/blog/recommendation-for-fortinet-devices	T3
FortiOS 7.2.11 & 7.4.7 : r/fortinet - Reddit	https://www.reddit.com/r/fortinet/comments/1jzsu6r/fortios_7211_747/	T3
Known issues | FortiGate / FortiOS 7.2.11 - Fortinet Document Library	https://docs.fortinet.com/document/fortigate/7.2.11/fortios-release...	T3

Generated 2026-06-19 18:57 UTC by TJS Security Command Center