INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-19 13:48 UTC

FortiBleed: 74,000 Fortinet Credentials Exposed as Russian-Linked Actors Target Global Infrastructure

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0517
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Fortinet FortiGate firewalls, Fortinet VPN gateways, Fortinet FortiSandbox (specific version ranges not confirmed in source data, verify via FortiGuard PSIRT advisories)
Published	2026-06-19T02:47:55
Discovery Source	Rss

Executive Summary

A dataset of approximately 73,932 Fortinet firewall and VPN device credentials spanning 194 countries has been publicly exposed in an event dubbed 'FortiBleed.' CISA has confirmed active exploitation targeting government agencies and critical infrastructure operators globally. Organizations running Fortinet FortiGate or VPN gateway devices face immediate risk of unauthorized network access, lateral movement, and potential operational disruption if credentials are not rotated and devices are not hardened.

Technical Analysis

The FortiBleed credential exposure event involves approximately 73,932 Fortinet FortiGate firewall and VPN gateway devices across 194 countries. A Russian-speaking threat group (attribution low confidence, not formally confirmed) is alleged to have conducted over 1.16 billion brute-force and credential stuffing attempts (T1110, T1110.001, T1110.003) against more than 320,000 FortiGate targets to compile the dataset. No discrete CVE has been assigned; this is an operational credential exposure event. Applicable CWEs include CWE-522 (insufficiently protected credentials), CWE-916 (use of password hash with insufficient computational effort), CWE-255 (credentials management errors), and CWE-307 (improper restriction of excessive authentication attempts). Exposed credentials enable remote service exploitation (T1133), valid account abuse (T1078, T1078.001), remote service access (T1021), file and directory discovery (T1083), and credential access from unsecured stores (T1552). Specific version ranges for affected devices are not confirmed in available source data; consult FortiGuard PSIRT advisories at https://www.fortiguard.com/psirt for authoritative version scope.

The majority of affected devices remain internet-facing and operational, sustaining the active threat window. All technical specifics should be validated against FortiGuard PSIRT and CISA advisories before action.

Action Checklist

1. Step 1: Containment, Immediately audit all Fortinet FortiGate and VPN gateway devices for internet exposure. Restrict management interfaces and VPN endpoints to known-good IP ranges using firewall ACLs. Disable any accounts not required for current operations (NIST AC-2; CIS 5.3). Cross-reference your device list against the FortiBleed exposure dataset if available through your threat intelligence feed.
2. Step 2: Detection, Query authentication logs on all FortiGate and VPN gateway devices for high-volume failed login events (indicative of T1110 brute-force activity) and successful logins from unexpected source IPs or at unusual hours (indicative of T1078 valid account abuse). Enable and review FortiGate event logs for anomalous remote access sessions (T1133, T1021). Correlate with SIEM for lateral movement indicators post-authentication. Reference NIST AU-6 and CIS 8.2 for log review requirements. No confirmed IOC IPs or hashes are available in source data for this campaign.
3. Step 3: Eradication, Rotate all credentials on affected Fortinet devices immediately, including local admin accounts, VPN user accounts, and any service accounts (D3-CRO, Credential Rotation). Enforce MFA on all remote access and administrative interfaces where supported (NIST AC-17; CIS 6.3, 6.4, 6.5; D3-MFA). Implement account lockout and rate-limiting policies to address CWE-307 (NIST AC-7). Consult FortiGuard PSIRT advisories for any firmware updates addressing credential storage weaknesses. Apply configuration hardening per CIS 4.2 and CIS 4.7 (manage default accounts).
4. Step 4: Recovery, After credential rotation, verify no unauthorized accounts or backdoor accounts remain on affected devices (NIST AC-2; D3-LAM, Local Account Monitoring). Confirm MFA enforcement is active on all remote access paths. Monitor authentication logs continuously for 30 days post-remediation for re-exploitation indicators. Validate audit logging is fully operational across all FortiGate devices (NIST AU-2, AU-12; CIS 8.2). Confirm session termination policies are enforced (NIST AC-12).
5. Step 5: Post-Incident, Conduct a gap assessment against NIST AC-7 (brute-force lockout), AC-17 (remote access controls), and AU-6 (log review frequency) to identify control deficiencies this event exposed. Document findings and update the vulnerability management process (CIS 7.1, 7.2). Review the organization's asset inventory to ensure all Fortinet devices are tracked (CIS 1.1). Evaluate whether credential storage practices meet current standards and address CWE-522 and CWE-916 findings in the next policy review cycle.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal counsel, and regulatory contacts immediately if any FortiGate authentication log shows a successful login from an IP address not belonging to your organization during the FortiBleed exposure window, if any net-new admin or VPN account is discovered that was not provisioned by your team, or if downstream network telemetry indicates lateral movement from a segment accessible via the compromised VPN gateway — any of these conditions may trigger breach notification obligations under HIPAA, CISA reporting requirements for critical infrastructure operators, or state-level PII disclosure laws.

Recovery Notes	After credential rotation and MFA enforcement are confirmed, conduct a full review of firewall policy changes, BGP/routing table integrity, and any scheduled tasks or automation scripts that reference FortiGate service accounts, as Russian-linked threat actors in similar campaigns (e.g., Sandworm, APT28) have been observed persisting via modified network policies and scheduled configuration scripts rather than solely through credential reuse. Monitor FortiGate SSL-VPN authentication logs and management interface access logs daily for a minimum of 30 days, specifically flagging any login attempt using a username that appears in the FortiBleed dataset. Coordinate with upstream ISPs or your MSSP if volumetric reconnaissance or scanning activity against your FortiGate external IPs continues post-remediation, as this may indicate the threat actor is validating whether the credential rotation was complete.
Forensic Artifacts	FortiGate SSL-VPN authentication logs (`/var/log/sslvpn/` and GUI Log & Report > Events > VPN Events): look for `action=tunnel-up` events with source IPs not in your allowlist, usernames appearing in the FortiBleed dataset, or login timestamps clustering around the dataset's public disclosure date — these are the primary indicators of credential abuse in this campaign. | FortiGate administrator login audit trail (GUI Log & Report > Events > System Events, filtered on `action=login` for the admin interface): any successful admin GUI or SSH login from an unrecognized IP during the exposure window indicates direct device compromise beyond VPN credential abuse. | FortiGate running configuration backup (pre-remediation): compare against your known-good baseline using diff to detect unauthorized policy additions, new admin accounts, modified trusted-host lists on admin accounts, or SSL-VPN split-tunnel policy changes that could facilitate data exfiltration — these are the persistence artifacts this threat actor class typically plants. | Active session and connection table snapshot (`diagnose sys session list` output captured before containment): preserves the source IPs, destination ports, and session ages of all connections transiting the FortiGate at the moment of discovery, which is the only record of attacker C2 or lateral movement IPs if no upstream NetFlow collection is in place. | FortiGate DHCP and routing table state (`get router info routing-table all` and `diagnose ip arp list`): Russian-linked infrastructure operators in similar campaigns have modified static routes or policy-based routes to redirect traffic through attacker-controlled next-hops; capturing routing state before remediation preserves evidence of any such manipulation that credential rotation alone would not undo.

Per-Action IR Details

Step 1: Containment — Immediately audit all Fortinet FortiGate and VPN gateway devices for internet exposure. Restrict management interfaces and VPN endpoints to known-good IP ranges using firewall ACLs. Disable any accounts not required for current operations (NIST AC-2; CIS 5.3). Cross-reference your device list against the FortiBleed exposure dataset if available through your threat intelligence feed.

NIST Phase: Containment

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

Controls: NIST AC-2 (Account Management), NIST AC-4 (Information Flow Enforcement), CIS 5.3 (Disable Dormant Accounts), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run `curl -s https://api.shodan.io/shodan/host/search?query=product:FortiGate&key=` or use the free Shodan web interface to identify internet-exposed FortiGate management ports (443, 8443, 4433). Cross-reference results against your internal asset list manually. Use `iptables` or the FortiGate CLI (`config firewall address` / `config firewall policy`) to restrict administrative GUI access to a named-IP allowlist immediately. Disable inactive local VPN accounts via `config vpn ssl settings` and `config user local` in the FortiOS CLI.

Evidence: Before restricting ACLs or disabling accounts, capture current active session state from each FortiGate: run `diagnose sys session list` and `get vpn ssl monitor` to record all active SSL-VPN sessions including source IPs,

usernames, session durations, and tunnel IDs. Export FortiGate event logs (`/var/log/` via SSH or GUI Log & Report) covering the prior 90 days, as the exposed credential dataset has unknown age. Capture the full running config (`show full-configuration` or backup via GUI) to preserve the pre-remediation state for forensic comparison.

Step 2: Detection — Query authentication logs on all FortiGate and VPN gateway devices for high-volume failed login events (indicative of T1110 brute-force activity) and successful logins from unexpected source IPs or at unusual hours (indicative of T1078 valid account abuse). Enable and review FortiGate event logs for anomalous remote access sessions (T1133, T1021). Correlate with SIEM for lateral movement indicators post-authentication. Reference NIST AU-6 and CIS 8.2 for log review requirements. No confirmed IOC IPs or hashes are available in source data for this campaign.

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), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, extract FortiGate authentication logs via SSH and parse with bash: `grep -E 'action=login|action=tunnel-up' /var/log/fortigate.log | awk '{print $1,$2,$5,$7,$9}' | sort | uniq -c | sort -rn | head -50` to surface high-frequency login sources. For SSL-VPN specifically, query the FortiGate event log GUI filter: `Event Type = VPN, Sub-type = SSL-VPN, Action = tunnel-up/tunnel-down` and export to CSV. Load into Python pandas or a spreadsheet to pivot by source IP and username. Flag any source IP appearing in the FortiBleed exposure window (cross-reference login timestamps against the dataset disclosure date). Use Sigma rule `proc_creation_win_susp_remote_access_tools` adapted for FortiOS syslog if forwarding to a local syslog server.

Evidence: This step is read-only (log query) and does not alter live state, so no pre-capture is required before initiating queries. However, before any downstream containment action triggered by findings here, capture: FortiGate SSL-VPN session logs (`/var/log/sslvpn/`), FortiAuthenticator authentication records if in use, and the output of `diagnose debug application sslvpn -1` for any currently active tunnel details. Note that FortiGate local log storage is ring-buffered and may overwrite — prioritize log export to a write-once syslog destination immediately.

Step 3: Eradication — Rotate all credentials on affected Fortinet devices immediately, including local admin accounts, VPN user accounts, and any service accounts (D3-CRO — Credential Rotation). Enforce MFA on all remote access and administrative interfaces where supported (NIST AC-17; CIS 6.3, 6.4, 6.5; D3-MFA). Implement account lockout and rate-limiting policies to address CWE-307 (NIST AC-7). Consult FortiGuard PSIRT advisories for any firmware updates addressing credential storage weaknesses. Apply configuration hardening per CIS 4.2 and CIS 4.7 (manage default accounts).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-17 (Remote Access), NIST AC-7 (Unsuccessful Logon Attempts), 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 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

Compensating: Enumerate all local FortiGate admin accounts via `config system admin` / `show system admin` and all VPN users via `config user local` / `show user local` before rotation. Use FortiOS CLI to set new passwords: `edit ` / `set password `. For MFA without an enterprise SSO, enable FortiToken Mobile (free for up to 2 tokens on FortiGate) via `config user fortitoken` or configure TOTP via a free RADIUS server (FreeRADIUS) integrated with FortiGate. Enable login lockout via `config system global` / `set admin-lockout-threshold 3` / `set admin-lockout-duration 300`.

Evidence: CRITICAL — volatile capture required before credential rotation alters live state. Before executing any password changes or account disablement: capture full output of `get vpn ssl monitor` (active tunnel usernames and source IPs), `diagnose sys session list` (established firewall sessions), and `get system performance status` (memory/CPU baseline to detect any persistent process anomaly). Export complete FortiGate config backup. If any administrative session is currently active from an unrecognized IP, capture that session's source IP, timestamp, and username before terminating — this is your highest-value indicator for threat actor attribution in this campaign.

Step 4: Recovery — After credential rotation, verify no unauthorized accounts or backdoor accounts remain on affected devices (NIST AC-2; D3-LAM — Local Account Monitoring). Confirm MFA enforcement is active on all remote access paths. Monitor authentication logs continuously for 30 days post-remediation for re-exploitation indicators. Validate audit logging is fully operational across all FortiGate devices (NIST AU-2, AU-12; CIS 8.2). Confirm session termination policies are enforced (NIST AC-12).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AC-12 (Session Termination), NIST AU-2 (Event Logging), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 8.2 (Collect Audit Logs)

Compensating: After rotation, re-run `show system admin` and `show user local` and compare the output line-count and usernames against your pre-incident config backup using `diff` to detect any net-new accounts the threat actor may have created during a confirmed access window. For continuous 30-day monitoring without a SIEM, configure FortiGate syslog forwarding (`config log syslogd setting`) to a local Linux syslog server (rsyslog) and write a daily cron job that greps for `action=login status=success` events and emails the results for manual review. Verify session timeout via `config vpn ssl settings` / `get idle-timeout`.

Evidence: This recovery verification step is read-only for most checks; however, if any net-new unauthorized account is discovered during verification, treat it as evidence of a confirmed threat actor persistence mechanism — capture the account's full attribute set (`edit ` / `show`) including creation timestamp, password hash if retrievable, and any associated trusted hosts before removing it. Preserve the diff output between pre- and post-incident config backups as a forensic record. Document all verified account states with timestamps for regulatory notification purposes.

Step 5: Post-Incident — Conduct a gap assessment against NIST AC-7 (brute-force lockout), AC-17 (remote access controls), and AU-6 (log review frequency) to identify control deficiencies this event exposed. Document findings and update the vulnerability management process (CIS 7.1, 7.2). Review the organization's asset inventory to ensure all Fortinet devices are tracked (CIS 1.1). Evaluate whether credential storage practices meet current standards and address CWE-522 and CWE-916 findings in the next policy review cycle.

NIST Phase: Post Incident

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

Controls: NIST AC-7 (Unsuccessful Logon Attempts), NIST AC-17 (Remote Access), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Produce a written gap assessment using the FortiGate audit checklist from CIS Benchmark for Fortinet FortiOS (available free via CIS website after registration). Specifically document whether admin lockout thresholds (AC-7) were configured before this event, whether VPN access was restricted to known-good IP ranges (AC-17), and whether log review was occurring on a defined schedule (AU-6). Use the asset inventory gap to drive a Shodan re-scan of your IP ranges for any FortiGate devices not in your CMDB. Submit findings to FortiGuard PSIRT via their disclosure portal if credential storage weaknesses are confirmed in your firmware version.

Evidence: No volatile evidence capture is required at this phase; all live state has been remediated. Preserve as long-term forensic records: the original pre-incident FortiGate config backup, the full authentication log export covering the FortiBleed disclosure window, the account diff output from Step 4, and any active session captures from Step 3. These records support breach notification obligations if unauthorized access to protected data is confirmed, and provide the before/after evidence baseline for the lessons-learned report.

Detection Guidance

Search FortiGate event logs and SIEM ingestion pipelines for the following indicators: (1) Excessive failed authentication events against management interfaces or SSL-VPN portals from single or rotating source IPs, consistent with T1110 brute-force and T1110.003 password spraying. (2) Successful authentication events from

IP addresses not in known-good baselines, particularly from anonymizing infrastructure or unexpected geographies. (3) Authentication events outside normal business hours on accounts that have no after-hours activity history, indicative of T1078 valid account abuse. (4) Log entries reflecting file or directory enumeration activity (T1083) or lateral movement via remote services (T1021) immediately following successful VPN authentication. (5) Any access to credential stores or configuration export functions (T1552) by accounts that do not normally perform those actions. Align log collection and retention with NIST AU-2, AU-3, AU-6, AU-11, and CIS 8.2. No confirmed campaign-specific IOCs (IP addresses, domains, hashes) are available in the source data provided; monitor threat intelligence feeds and FortiGuard PSIRT for updates. All detection findings should be escalated to incident response for triage given CISA's active exploitation confirmation.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`no confirmed IOCs available in source data`	No campaign-specific IP addresses, domains, or file hashes were confirmed in the provided source material. Monitor FortiGuard PSIRT and CISA advisories for IOC updates as the investigation matures.	LOW

Framework Mappings

MITRE-ATTACK

- **T1021** — Remote Services
- **T1110.003** — Password Spraying
- **T1083** — File and Directory Discovery
- **T1133** — External Remote Services
- **T1110** — Brute Force
- **T1552** — Unsecured Credentials
- **T1110.001** — Password Guessing
- **T1078.001** — Default Accounts
- **T1589** — Gather Victim Identity Information
- **T1589.001** — Credentials
- **T1654** — Log Enumeration
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **IA-2** — Identification and Authentication (Organizational Users)
- **AC-20** — Use of External Systems

- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **AC-7** — Unsuccessful Logon Attempts
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **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
- **5.2** — Use Unique Passwords

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

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

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1021	Remote Services	Lateral-Movement
T1110.003	Password Spraying	Credential-Access
T1083	File and Directory Discovery	Discovery
T1133	External Remote Services	Persistence
T1110	Brute Force	Credential-Access
T1552	Unsecured Credentials	Credential-Access
T1110.001	Password Guessing	Credential-Access

Technique ID	Technique Name	Tactic
T1078.001	Default Accounts	Defense-Evasion
T1589	Gather Victim Identity Information	Reconnaissance
T1589.001	Credentials	Reconnaissance
T1654	Log Enumeration	Discovery
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/cisa-warns-fortinet-...	T3
	https://www.bleepingcomputer.com/news/security/cisa-warns-fortinet-...	T3
Fortinet "FortiBleed" Global Compromise & Active Exploitation of ...	https://kudelskisecurity.com/research/fortinet-fortibleed-global-co...	T3
Active FortiBleed Campaign Impacting Fortinet Devices Across 194 ...	https://arcticwolf.com/resources/blog/active-fortibleed-campaign-im...	T3
PSIRT Advisories - FortiGuard Labs	https://www.fortiguard.com/psirt	T3

Generated 2026-06-19 13:48 UTC by TJS Security Command Center