INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 14:15 UTC

FortiBleed: Mass Credential Leak Exposes VPN Access for ~74,000 Fortinet Devices

DATA BREACH | **CRITICAL** | CVSS 9.1

SCC Item ID	SCC-DBR-2026-0181
Type	Data Breach
Severity	CRITICAL
CVSS Base Score	9.1
Affected Products	Fortinet FortiGate firewalls and SSL-VPN infrastructure (specific firmware versions unconfirmed from available sources)
Discovery Source	Gemini

Executive Summary

A credential leak event dubbed 'FortiBleed' reportedly exposed VPN usernames, passwords, and configuration files from approximately 74,000 Fortinet FortiGate firewall and SSL-VPN devices. The credentials are believed harvested via previously disclosed authentication bypass vulnerabilities in FortiGate SSL-VPN, with a confirmed post-exploitation symlink persistence technique (Fortinet PSIRT FG-IR-25-934) indicating adversaries may retain access even on devices that have since been patched. Organizations running Fortinet perimeter devices face immediate risk of unauthorized network access, lateral movement, and data exfiltration if affected credentials have not been rotated.

Technical Analysis

The FortiBleed incident involves a reported mass credential leak from FortiGate devices. The exact scale (74,000 devices) is reported but not independently confirmed by CISA or NVD as of this writing. However, the underlying technical context - CVE-2025-59718 exploitation, Fortinet PSIRT FG-IR-25-934 symlink persistence, and active VPN credential harvesting campaigns - is documented in authoritative sources and represents confirmed, actionable risk.

Relevant technical context from available sources:

1. CVE-2025-59718 (CWE-288, Authentication Bypass Using Alternate Path): An authentication bypass vulnerability in FortiGate reported as exploited in the wild as of December 2025 (HelpNetSecurity). This is a network-accessible, unauthenticated exploitation path consistent with mass credential harvesting. CVSS base score provided in item data: 9.1. Vendor CVSS not confirmed in available sources.

2. FG-IR-25-934, SSL-VPN Symlink Persistence (Fortinet PSIRT, CISA advisory April 11 2025): Adversaries exploiting FortiGate SSL-VPN vulnerabilities planted symlinks in the SSL-VPN filesystem that survived firmware upgrades, allowing read access to system files from the SSL-VPN web management interface post-patch. This technique means patching alone does not guarantee remediation if the symlink artifact persists.

3. MITRE ATT&CK techniques mapped: T1190 (Exploit Public-Facing Application), T1133 (External Remote Services, SSL-VPN), T1078 (Valid Accounts, use of stolen VPN credentials), T1552 (Unsecured Credentials, configuration file exposure), T1530 (Data from Cloud Storage, configuration exfiltration).

4. CWE references: CWE-200 (Exposure of Sensitive Information), CWE-288 (Authentication Bypass), CWE-522 (Insufficiently Protected Credentials).

Affected firmware versions are unconfirmed from available sources. Fortinet's official PSIRT advisory (FG-IR-25-934) and the FortiGuard Labs portal are the authoritative references for version-specific impact. No specific IOCs (IPs, hashes, domains) are confirmed in the available source material.

Action Checklist

1. Step 1: Containment. Immediately audit all FortiGate SSL-VPN devices for the symlink persistence artifact described in Fortinet PSIRT advisory FG-IR-25-934. Per the CISA April 2025 advisory, restrict SSL-VPN management interface access to trusted IP ranges and disable SSL-VPN on devices that cannot be immediately inspected. Apply NIST AC-17 (Remote Access) controls: review and enforce documented usage restrictions for all remote access paths.
2. Step 2: Detection. Review FortiGate authentication logs for anomalous VPN logins, especially off-hours access, logins from unexpected geographies, or concurrent sessions from different source IPs for the same account (NIST AU-6, AU-12; CIS 8.2). Query SIEM for T1078 indicators: successful authentications followed immediately by internal reconnaissance or lateral movement. Check SSL-VPN filesystem for unexpected symlinks per FG-IR-25-934 indicators. Apply D3-LAM (Local Account Monitoring) to flag dormant or service accounts authenticating to VPN. No confirmed IOC values are available from current sources to include in blocklists.
3. Step 3: Eradication. Rotate all VPN credentials for FortiGate SSL-VPN users immediately, treating all credentials on affected device generations as compromised. Apply the Fortinet FG-IR-25-934 remediation steps to remove symlink artifacts (consult https://fortiguard.fortinet.com/psirt/FG-IR-25-934 directly; do not rely on patching alone, as symlink artifacts may persist after firmware updates). Apply available patches for CVE-2025-59718 per Fortinet's official advisory. Enforce D3-CRO (Credential Rotation) and D3-CH (Credential Hardening). Reference CIS 5.2 (Use Unique Passwords) and CIS 6.3 (Require MFA for Externally-Exposed Applications).
4. Step 4: Recovery. After credential rotation and patch application, validate that no symlink artifacts remain per FG-IR-25-934 guidance. Monitor VPN authentication logs for 30 days post-remediation for re-use of rotated credentials, which would indicate credential reuse by an actor who pre-staged access. Enable MFA on all SSL-VPN access per CIS 6.4 (Require MFA for Remote Network Access) and D3-MFA. Validate firewall rules restrict SSL-VPN management to approved source IPs (NIST AC-3, AC-17).
5. Step 5: Post-Incident. Conduct a lessons-learned review focused on three control gaps this event exposed: (1) Credential storage and protection on network perimeter devices (NIST IA controls, CWE-522); (2) Patch verification processes that confirm persistence artifacts are removed, not only that firmware is updated (Fortinet PSIRT FG-IR-25-934 specifically demonstrates patching without artifact

removal is insufficient); (3) MFA coverage gaps on external-facing VPN infrastructure (CIS 6.3, 6.4, 6.5). Update incident response playbooks to include FortiGate-specific persistence checks as a standard step for any FortiGate-involved incident.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal counsel, and privacy/compliance officers immediately if any post-rotation VPN authentication succeeds using pre-rotation credentials (indicating active adversary access), if SSL-VPN IP pool addresses are observed initiating internal lateral movement, if PII or regulated data (PHI, PCI) is accessible via the compromised VPN segment, or if the organization lacks the capability to audit all ~74,000 potentially affected FortiGate devices within a 24-hour window.
Recovery Notes	Following credential rotation, symlink removal per FG-IR-25-934, and patch application, validate recovery by running 'find /data -type l 2>/dev/null' on every remediated device and confirming zero output against the documented pre-remediation baseline. Maintain enhanced VPN authentication log review for a minimum of 30 days, specifically hunting for authentication patterns from the geographic regions, ASNs, or time windows identified during the detection phase as anomalous — credential reuse by a pre-staged actor is the primary residual risk. Do not declare recovery complete on any device until both the firmware version and the symlink artifact check are documented in writing, as FG-IR-25-934 explicitly establishes that patching alone is insufficient.
Forensic Artifacts	FortiGate SSL-VPN authentication event logs (Log & Report > VPN Events; syslog category 'event' subtype 'vpn'): records successful and failed authentications with source IP, username, and session duration — the primary artifact for identifying credential abuse from the leaked FortiBleed dataset | FortiGate filesystem symlink enumeration output ('find /data -type l 2>/dev/null' and 'ls -la /data/lib/'): documents the FG-IR-25-934 persistence artifact — unexpected symlinks pointing into root filesystem locations outside /data/lib/ are direct evidence of post-exploitation persistence on a device that may appear patched | FortiGate active SSL-VPN session table ('get vpn ssl monitor'): volatile in-memory state capturing all authenticated tunnel endpoints, usernames, and source IPs at the moment of containment — destroyed on SSL-VPN service restart or device reboot | FortiGate configuration backup (pre-remediation, exported via 'execute backup config tftp'): preserves the device configuration state at time of incident including admin trusted-host settings, SSL-VPN realm configuration, and local user accounts — required for forensic and legal chain-of-custody | Internal network traffic logs from the SSL-VPN IP address pool (firewall forward traffic logs, NetFlow, or perimeter PCAP): identifies post-authentication lateral movement from compromised VPN sessions into internal segments — the key artifact for determining blast radius beyond the VPN device itself

Per-Action IR Details

Step 1: Containment — Immediately audit all FortiGate SSL-VPN devices for the symlink persistence artifact described in FG-IR-25-934. Per the CISA April 2025 advisory, restrict SSL-VPN management interface access to trusted IP ranges and disable SSL-VPN on devices that cannot be immediately inspected. Apply NIST AC-17 (Remote Access) controls: review and enforce documented usage restrictions for all remote access paths.

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

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: For teams without centralized management: use FortiGate CLI command 'get vpn ssl settings' and 'diagnose sys mount list' on each device to enumerate active SSL-VPN configurations and detect unexpected symlink mounts under /data/lib/. Use a two-person checklist process — one analyst runs commands, the second documents output — to audit each device serially. Restrict management access by editing trusted host fields under each admin account via CLI: 'config system admin; edit ; set trusthost1 '.

Evidence: Before restricting access or disabling SSL-VPN, capture: (1) full output of 'diagnose sys mount list' and 'ls -la /data/lib/' to document symlink presence; (2) active SSL-VPN session table via 'get vpn ssl monitor' to record all authenticated sessions, source IPs, and usernames at time of containment; (3) FortiGate event log snapshot (Log & Report > Events > VPN Events) covering at minimum the prior 90 days, exported before any configuration change. These are volatile or potentially overwritten once sessions are terminated or the device is reconfigured.

Step 2: Detection — Review FortiGate authentication logs for anomalous VPN logins, especially off-hours access, logins from unexpected geographies, or concurrent sessions from different source IPs for the same account (NIST AU-6, AU-12; CIS 8.2). Query SIEM for T1078 indicators: successful authentications followed immediately by internal reconnaissance or lateral movement. Check SSL-VPN filesystem for unexpected symlinks per FG-IR-25-934 indicators. Apply D3-LAM (Local Account Monitoring) to flag dormant or service accounts authenticating to VPN. No confirmed IOC values are available from current sources to include in blocklists.

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

Compensating: Without a SIEM: export FortiGate VPN event logs (Log & Report > VPN Events, or via CLI 'execute log filter category event; execute log display') to CSV and process with PowerShell: 'Import-Csv vpn_events.csv | Where-Object { $_.action -eq "ssl-login" } | Group-Object user | Sort-Object Count -Descending' to identify accounts with unusually high login volume or multiple source IPs. Cross-reference authentication timestamps against business-hours baseline manually. For symlink detection, SSH to each FortiGate and run 'find /data -type l 2>/dev/null' — any symlinks in unexpected paths (e.g., pointing outside /data/lib/ into root filesystem locations) should be flagged immediately.

Evidence: Capture before any session invalidation or log rotation: (1) FortiGate SSL-VPN authentication logs (fgd_event.log or syslog forwarded records) showing successful and failed logins with source IP, username, and timestamp; (2) 'get vpn ssl monitor' session table output capturing active tunnel endpoints; (3) FortiGate traffic logs (forward traffic log) for sessions originating from SSL-VPN IP pool addresses to identify post-authentication lateral movement; (4) output of 'diagnose debug application sslvpn -1' if logging verbosity was elevated — this may contain session tokens. Volatile state (active sessions, in-memory session table) is lost immediately upon SSL-VPN service restart or device reboot.

Step 3: Eradication — Rotate all VPN credentials for FortiGate SSL-VPN users immediately, treating all credentials on affected device generations as compromised. Apply the FortiGuard FG-IR-25-934 remediation steps to remove symlink artifacts (consult https://fortiguard.fortinet.com/psirt/FG-IR-25-934 directly — do not rely on patching alone). Apply available patches for CVE-2025-59718 per Fortinet's official advisory. Enforce D3-CRO (Credential Rotation) and D3-CH (Credential Hardening). Reference CIS 5.2 (Use Unique Passwords) and CIS 6.3 (Require MFA for Externally-Exposed Applications).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), CIS 5.2 (Use Unique Passwords), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: For credential rotation without an IAM platform: use FortiGate CLI to reset all local VPN user passwords in batch — 'config user local; edit ; set passwd ' — and generate passwords using a local password manager (Bitwarden, KeePass) to ensure uniqueness per CIS 5.2. For LDAP-integrated environments, force an AD password reset via PowerShell: 'Get-ADUser -Filter * -SearchBase "OU=VPN_Users,DC=domain,DC=com" | Set-ADAccountPassword -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "" -Force)'. Verify symlink removal by re-running 'find /data -type l 2>/dev/null' post-remediation and comparing against the pre-remediation baseline captured in Step 1.

Evidence: Before rotating credentials or applying the FG-IR-25-934 remediation: (1) take a final snapshot of 'get vpn ssl monitor' to confirm no active adversary sessions that would be disrupted and alerted; (2) document all symlink paths found (full 'ls -la' output from /data/lib/ and any other identified paths) as forensic record of the persistence mechanism; (3) preserve FortiGate configuration backup ('execute backup config tftp ') in its pre-remediation state for forensic and legal chain-of-custody purposes; (4) if firmware update is part of remediation, capture current firmware version ('get system status') before upgrade to confirm the specific affected build is recorded.

Step 4: Recovery — After credential rotation and patch application, validate that no symlink artifacts remain per FG-IR-25-934 guidance. Monitor VPN authentication logs for 30 days post-remediation for re-use of rotated credentials, which would indicate credential reuse by an actor who pre-staged access. Enable MFA on all SSL-VPN access per CIS 6.4 (Require MFA for Remote Network Access) and D3-MFA. Validate firewall rules restrict SSL-VPN management to approved source IPs (NIST AC-3, AC-17).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-3 (Access Enforcement), NIST AC-17 (Remote Access), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Without enterprise MFA: deploy FortiAuthenticator (free-tier or trial) or integrate FortiGate SSL-VPN with a TOTP-based solution (e.g., FreeRADIUS + Google Authenticator) as a compensating control pending full MFA rollout. For post-recovery monitoring without SIEM, schedule a daily cron job or Task Scheduler task to export FortiGate VPN logs and run a diff against a baseline of known-good credentials: flag any authentication attempt using a username/password combination that matches the pre-rotation credential set (pattern-match against hashed baseline). Review trusted host restrictions on all FortiGate admin accounts weekly for the 30-day watch period using CLI 'show system admin'.

Evidence: Recovery validation artifacts to document and retain: (1) post-remediation 'find /data -type l 2>/dev/null' output confirming zero symlinks — compare byte-for-byte against pre-remediation capture; (2) FortiGate firmware version post-patch ('get system status') confirming the specific build addressed by FG-IR-25-934; (3) MFA enrollment confirmation records for all SSL-VPN user accounts; (4) firewall policy export showing trusted-host restrictions applied to management interface — retain as configuration baseline. Any authentication event during the 30-day watch period using a credential matching the pre-rotation format should be treated as active compromise and trigger re-escalation to containment.

Step 5: Post-Incident — Conduct a lessons-learned review focused on three control gaps this event exposed: (1) Credential storage and protection on network perimeter devices (NIST IA controls, CWE-522); (2) Patch verification processes that confirm persistence artifacts are removed, not only that firmware is updated (FG-IR-25-934 specifically demonstrates patching without artifact removal is insufficient); (3) MFA coverage gaps on external-facing VPN infrastructure (CIS 6.3, 6.4, 6.5). Update incident response playbooks to include FortiGate-specific persistence checks as a standard step for any FortiGate-involved incident.

NIST Phase: Post Incident

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

Controls: CIS 6.3 (Require MFA for Externally-Exposed Applications), 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: For teams without a formal GRC platform: document lessons-learned in a shared markdown file or wiki page with three required sections mapped to the gaps above. For patch verification, add a mandatory CLI

validation step to the patch runbook: after every FortiGate firmware update, technician must run 'find /data -type l 2>/dev/null' and record output — a non-empty result is a failed remediation regardless of firmware version. Publish a one-page FortiGate Persistence Artifact Quick Reference card (covering FG-IR-25-934 symlink paths, relevant CLI commands, and expected clean-state output) for on-call responders.

Evidence: Post-incident documentation artifacts to compile and retain: (1) timeline reconstruction from FortiGate VPN logs mapping first anomalous authentication to containment action — this establishes dwell time and is required for breach notification assessment; (2) before-and-after configuration exports showing management access restrictions and MFA enforcement status; (3) full symlink artifact inventory (paths, link targets, creation timestamps where recoverable) as evidence of the FG-IR-25-934 persistence mechanism; (4) credential rotation completion records with timestamps for all affected accounts — required to bound the credential exposure window for regulatory and legal purposes.

Detection Guidance

Priority detection actions based on available source material:

1. VPN Authentication Anomalies (NIST AU-6, AU-12; CIS 8.2): Query authentication logs for FortiGate SSL-VPN for successful logins outside business hours, from unexpected source geographies, or using accounts inactive for more than 45 days (CIS 5.3). Concurrent sessions from distinct source IPs for a single account are a high-priority indicator of credential reuse (T1078).

2. Symlink Persistence Artifact (Fortinet PSIRT FG-IR-25-934): Per the CISA April 2025 advisory and FortiGuard Labs, inspect the SSL-VPN filesystem for unexpected symbolic links that provide read access to system files via the web management interface. This is a manual or scripted filesystem check, not a log-based detection. Apply D3-SFA (System File Analysis).

3. Post-Authentication Lateral Movement (T1078, T1133): Correlate successful VPN authentications with subsequent internal network scanning, SMB enumeration, or credential dumping activity within 15 minutes of login. This behavioral chain, documented in Darktrace's FortiGate SSL-VPN analysis, indicates exploitation beyond initial access.

4. Configuration File Exfiltration (T1552, T1530): Alert on large outbound transfers from FortiGate management interfaces or any out-of-band access to configuration backup files. Apply D3-UAP (User Account Permissions) to restrict who can export device configuration.

Note: No confirmed IOC values (IPs, domains, file hashes) from this specific FortiBleed event are available in the current source material. Do not populate blocklists with unverified values. Monitor Fortinet PSIRT and CISA for updated IOC releases.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs available`	No specific IP addresses, domains, or file hashes associated with the FortiBleed credential leak event have been confirmed in available source material. Do not populate blocklists from unverified community claims. Monitor Fortinet PSIRT and CISA for official IOC releases.	LOW

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage
- **T1133** — External Remote Services
- **T1078** — Valid Accounts
- **T1552** — Unsecured Credentials
- **T1190** — Exploit Public-Facing Application

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
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication
- **164.312(e)(1)** — Transmission Security

CIS-V8

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

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
T1530	Data from Cloud Storage	Collection
T1133	External Remote Services	Persistence
T1078	Valid Accounts	Defense-Evasion
T1552	Unsecured Credentials	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Tracking and Containing a Real-World Fortinet SSL-VPN Attack	https://www.darktrace.com/blog/from-exploit-to-escalation-tracking-...	T3
Faith in Fortinet? : r/networking - Reddit	https://www.reddit.com/r/networking/comments/1bfm16p/faith_in_forti...	T3
Fortinet Releases Advisory on New Post-Exploitation Technique for ...	https://www.cisa.gov/news-events/alerts/2025/04/11/fortinet-release...	T1

Source	URL	Tier
SSL-VPN Symlink Persistence Patch Bypass - FortiGuard Labs	https://fortiguard.fortinet.com/psirt/FG-IR-25-934	T3
Attackers are exploiting auth bypass vulnerability on FortiGate ...	https://www.helpnetsecurity.com/2025/12/17/fortigate-vulnerability-...	T3

Generated 2026-06-18 14:15 UTC by TJS Security Command Center