INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-17 18:49 UTC

FortiBleed: ~73,000 FortiGate Credentials Exposed Across Half the Internet-Facing Fortinet Population

DATA BREACH | CRITICAL | CVSS 9.5

SCC Item ID	SCC-DBR-2026-0178
Type	Data Breach
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Fortinet FortiGate SSL VPN, FortiOS (specific versions not confirmed in source data)
Published	2026-06-17T11:12:57
Discovery Source	Rss

Executive Summary

A dataset called 'FortiBleed' has exposed SSL VPN credentials for approximately 73,932 FortiGate devices across 194 countries, with independent researchers confirming the data is authentic. An alleged Russian-speaking threat group conducted roughly 1.16 billion brute-force attempts, cracked recovered authentication hashes using a 45-GPU cluster, and used the resulting credentials to move laterally into Active Directory environments. Organizations running internet-facing FortiGate SSL VPN appliances face immediate risk of unauthorized network access, domain compromise, and cascading breach of internal systems, with remediation scope unclear because the initial compromise vector has not been confirmed.

Technical Analysis

The 'FortiBleed' dataset contains SSL VPN credentials for approximately 73,932 FortiGate devices. Specific affected FortiOS versions are not confirmed in available source data. No CVE has been attributed to the initial extraction vector; the root cause of the credential exposure remains unidentified as of discovery date. The attack chain, per BleepingComputer reporting (T3 source, corroboration from authoritative sources pending), involved large-scale brute-force authentication attempts (T1110.001, T1110.002, T1110.003) against internet-facing FortiGate SSL VPN endpoints (T1133), hash cracking via a reported 45-GPU cluster, and subsequent lateral movement into Active Directory using recovered credentials (T1078, T1078.002, T1021.002). Post-compromise activity includes credential dumping (T1003), file discovery (T1083), and data collection (T1005). References to Microsoft SQL Server in source materials reflect lateral movement targets, not an initial attack surface. Relevant CWEs: CWE-255 (credentials management errors), CWE-287 (improper authentication), CWE-522

(insufficiently protected credentials), CWE-200 (exposure of sensitive information). Threat actor attribution to a Russian-speaking group is alleged at low confidence with no authoritative confirmation. Source quality score is 0.64; exploitation details require corroboration from Fortinet PSIRT and CISA before treating any specific technical claim as confirmed.

Action Checklist

1. Step 1: Containment, Immediately audit all internet-facing FortiGate SSL VPN appliances; restrict VPN access to known IP ranges where operationally feasible. Disable or rotate all SSL VPN local accounts and service accounts pending investigation. Check Fortinet PSIRT (https://www.fortinet.com/blog/psirt, search-retrieved, recommend human validation) for any published advisory on this dataset; no confirmed advisory was available in source data at time of writing.
2. Step 2: Detection, Query firewall and VPN authentication logs for high-volume failed login sequences followed by successful authentication from unexpected source IPs (NIST AU-6, CIS 8.2). Search Active Directory logs for anomalous account activity, new privileged account creation, and lateral movement indicators (event IDs 4624, 4625, 4648, 4768, 4769, 4776) occurring after any FortiGate VPN authentication event. Review for T1133 (external remote services) and T1078.002 (valid domain accounts) activity patterns in your SIEM.
3. Step 3: Eradication, Rotate all FortiGate SSL VPN credentials and any Active Directory credentials that could have been exposed via lateral movement (NIST AC-2, D3-CRO). Disable and audit all local VPN accounts; enforce MFA on all SSL VPN authentication paths (NIST AC-17, CIS 6.4, D3-MFA). Apply the current Fortinet-recommended FortiOS version per official Fortinet PSIRT guidance once an advisory is published; no specific patch ID is confirmed in available source data, do not apply speculative versions.
4. Step 4: Recovery, Verify no unauthorized accounts, scheduled tasks, or persistence mechanisms remain in Active Directory or on FortiGate appliances (D3-LAM, D3-SICA). Confirm SSL VPN authentication is logging correctly and alerts are firing on anomalous access patterns (NIST AU-2, AU-12). Monitor VPN and AD environments continuously for 30 days post-remediation for indicators of re-compromise given the unconfirmed initial vector.
5. Step 5: Post-Incident, Conduct a control gap review against NIST AC-7 (failed logon lockout thresholds), AC-17 (remote access policy), and CIS 7.1 (vulnerability management process) to assess whether brute-force lockout policies were enforced. Evaluate whether internet-facing VPN endpoints were included in your active attack surface inventory (CIS 1.1). Establish a process to monitor Fortinet PSIRT and CISA KEV for future advisories related to this event; subscribe to Fortinet's security advisory feed.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal, privacy counsel, and executive leadership if forensic review confirms that any Active Directory accounts traversed by the threat group had access to PII, PHI, or payment card data — 73,932 devices across 194 countries and confirmed credential cracking with AD lateral movement likely triggers breach notification obligations under GDPR, HIPAA, and/or state privacy statutes depending on organizational scope.

Recovery Notes	Given that the threat group used cracked VPN credentials to move laterally into Active Directory environments, recovery cannot be declared complete until a full privileged account audit confirms no backdoor accounts or persistent access mechanisms remain in AD or on FortiGate appliances. Monitor FortiGate SSL VPN authentication logs and AD Security Event Logs continuously for a minimum of 30 days post-remediation, with specific focus on any authentication originating from the same source IP ranges observed during the incident. Treat any re-appearance of previously-observed attacker source IPs or credential reuse patterns as an active re-compromise requiring immediate return to containment phase.
Forensic Artifacts	FortiGate SSL VPN event logs (/var/log/ on-appliance, or Log & Report > VPN Events in GUI): filter for 'action=tunnel-up' events preceded by high-volume 'status=failed' from the same source IP — the 1.16 billion brute-force pattern would produce a distinctive failure spike immediately before each successful tunnel establishment | Active Directory Security Event Log on all domain controllers: Event ID 4768/4769 (Kerberos ticket requests) and 4624 Logon Type 3 (network logons) timestamped within minutes of FortiGate VPN tunnel-up events from unexpected IPs, indicating the threat group's credential-to-lateral-movement pivot using cracked FortiGate hashes | FortiGate running configuration backup ('execute backup config'): compare against known-good baseline to identify attacker-added local admin accounts, modified SSL VPN split-tunnel policies, or rogue authentication servers added to persist access beyond initial credential use | Windows Security Event Log Event ID 4720 (account created), 4732 (member added to security-enabled local group), and 4756 (member added to universal security group) on domain controllers: these would reflect the threat group creating backdoor privileged accounts after using cracked FortiGate credentials to authenticate to AD | NetFlow or FortiGate firewall session logs showing outbound connections from internal hosts that authenticated via compromised VPN credentials: lateral movement from FortiGate into AD environments would produce internal east-west traffic patterns (SMB/445, LDAP/389, RDP/3389, WinRM/5985) that are anomalous for those source hosts during the compromise window

Per-Action IR Details

Step 1: Containment — Immediately audit all internet-facing FortiGate SSL VPN appliances; restrict VPN access to known IP ranges where operationally feasible. Disable or rotate all SSL VPN local accounts and service accounts pending investigation. Check Fortinet PSIRT (https://www.fortinet.com/blog/psirt — search-retrieved, recommend human validation) for any published advisory on this dataset; no confirmed advisory was available in source data at time of writing.

NIST Phase: Containment

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

Controls: NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 6.2 (Establish an Access Revoking Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Without a SIEM, enumerate all FortiGate local VPN accounts via CLI: 'get user local' and 'get vpn ssl monitor'. Immediately disable non-essential accounts with 'config user local / edit / set status disable / end'. Restrict SSL VPN source IPs via FortiGate policy: 'config firewall policy' — add a source address group containing only known corporate egress IPs and apply to the SSL VPN portal policy. Document all changes with timestamps for the incident record.

Evidence: Before disabling or rotating any FortiGate SSL VPN account, capture: (1) current active SSL VPN sessions via 'diagnose vpn ssl list' — pipe to file; (2) FortiGate traffic logs from /var/log/ for the preceding 72 hours showing source IPs and authenticated usernames; (3) 'diagnose debug application sslvpn -1' output if live sessions are active; (4) FortiGate event logs (type=event subtype=vpn) showing authentication successes from unexpected geographies or IPs. These are volatile — active sessions and in-memory state are destroyed the moment accounts are disabled or the appliance is restarted.

Step 2: Detection — Query firewall and VPN authentication logs for high-volume failed login sequences followed by successful authentication from unexpected source IPs (NIST AU-6, CIS 8.2). Search Active Directory logs for anomalous account activity, new privileged account creation, and lateral movement indicators (event IDs 4624, 4625, 4648, 4768, 4769, 4776) occurring after any FortiGate VPN authentication event. Review for T1133 (external remote services) and T1078.002 (valid domain accounts) activity patterns in your SIEM.

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, use PowerShell on the AD domain controller to query the Security event log: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4624,4625,4648,4768,4769,4776)} | Select-Object TimeCreated,Id,Message | Export-Csv ad_auth_events.csv'. Cross-reference successful logins (4624 Logon Type 3 or 10) with the timestamp window of FortiGate VPN authentications by comparing the FortiGate event log exports. For brute-force detection on FortiGate without a SIEM, parse exported logs with: 'grep "action=tunnel-up\|action=tunnel-down\|status=failed" fortios_vpn.log | awk '{print $5}' | sort | uniq -c | sort -rn' to surface source IPs with high failure-to-success ratios consistent with the reported 1.16 billion brute-force pattern.

Evidence: Capture before any remediation action: (1) FortiGate SSL VPN authentication logs (Log & Report > VPN Events) covering at minimum the 90 days prior, filtered for 'action=tunnel-up' correlated with 'action=login-failed' from the same source IP within a 24-hour window — this matches the brute-force-then-success pattern used by this threat group; (2) Active Directory Security Event Log from all domain controllers, specifically Event ID 4768 (Kerberos TGT requests) and 4769 (Kerberos service ticket requests) timestamped within 15 minutes of any FortiGate VPN tunnel-up event from an unexpected IP — lateral movement via cracked credentials would produce this sequence; (3) AD objects for any accounts created or elevated to Domain Admins / Enterprise Admins after suspected compromise window (Event ID 4720, 4732, 4756).

Step 3: Eradication — Rotate all FortiGate SSL VPN credentials and any Active Directory credentials that could have been exposed via lateral movement (NIST AC-2, D3-CRO). Disable and audit all local VPN accounts; enforce MFA on all SSL VPN authentication paths (NIST AC-17, CIS 6.4, D3-MFA). Apply the current Fortinet-recommended FortiOS version per official Fortinet PSIRT guidance once an advisory is published; no specific patch ID is confirmed in available source data — do not apply speculative versions.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-17 (Remote Access), NIST SI-2 (Flaw Remediation), CIS 6.4 (Require MFA for Remote Network Access), CIS 5.2 (Use Unique Passwords), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: For credential rotation without enterprise tooling: export all FortiGate local users via 'get user local', generate unique passwords per account using 'openssl rand -base64 16', and apply via CLI batch. For AD accounts identified as potentially traversed by this threat group's lateral movement, use 'Set-ADAccountPassword' in PowerShell for bulk forced reset targeting accounts whose last logon timestamp aligns with the VPN compromise window. For MFA on FortiGate SSL VPN without a commercial IdP, configure FortiAuthenticator (free VM tier) with TOTP — or use FortiGate's built-in two-factor email token as an interim control pending full MFA deployment.

Evidence: Before rotating credentials or applying FortiOS updates, capture: (1) full RAM image of the FortiGate appliance if forensically feasible using vendor-supported diagnostic snapshot ('execute tac report') — cracked credential sessions and active tunnel metadata reside in memory; (2) complete 'diagnose sys session list' output showing all active firewall sessions that may reflect attacker-established persistent tunnels; (3) FortiGate configuration backup ('execute backup config ftp/tftp') before any change — the running config may contain attacker-added local accounts, modified SSL VPN policies, or rogue admin accounts created during lateral movement that will be overwritten by eradication actions; (4) AD snapshot of all privileged group memberships (Domain Admins, Enterprise Admins, Account Operators) before any account changes, as the threat group's AD lateral movement may have added

backdoor accounts.

Step 4: Recovery — Verify no unauthorized accounts, scheduled tasks, or persistence mechanisms remain in Active Directory or on FortiGate appliances (D3-LAM, D3-SICA). Confirm SSL VPN authentication is logging correctly and alerts are firing on anomalous access patterns (NIST AU-2, AU-12). Monitor VPN and AD environments continuously for 30 days post-remediation for indicators of re-compromise given the unconfirmed initial vector.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Run 'Get-ADUser -Filter * -Properties LastLogonDate,Enabled,MemberOf | Where-Object {$_.Enabled -eq $true -and $_.LastLogonDate -lt (Get-Date).AddDays(-45)}' to identify dormant AD accounts that may have been used as pivot accounts during lateral movement and were not flagged during detection. On FortiGate, verify no unexpected admin accounts exist: 'show system admin' — compare against a pre-incident baseline. Deploy Sysmon with SwiftOnSecurity's configuration on all AD-joined Windows hosts to log process creation (Event ID 1), network connections (Event ID 3), and scheduled task creation (Event ID 12/13) as a persistent monitoring layer for the 30-day watch period; forward to a centralized log file reviewable by the 2-person team.

Evidence: Before declaring recovery complete, collect and retain: (1) final FortiGate 'show full-configuration' diff against the last known-good configuration backup — any delta is a finding; (2) AD replication metadata report ('repadmin /showrepl') and a full export of all accounts created or modified during the incident window using 'Get-ADObject -Filter {WhenCreated -gt }'; (3) scheduled tasks on all AD domain controllers and any Windows hosts reachable from the VPN segment ('schtasks /query /fo LIST /v > schtasks_baseline.txt') — the threat group's AD lateral movement may have established persistence via scheduled tasks using domain credentials obtained from cracked FortiGate hashes; (4) NetFlow or firewall session logs confirming no outbound C2 traffic from hosts that authenticated via the compromised VPN credentials during the incident window.

Step 5: Post-Incident — Conduct a control gap review against NIST AC-7 (failed logon lockout thresholds), AC-17 (remote access policy), and CIS 7.1 (vulnerability management process) to assess whether brute-force lockout policies were enforced. Evaluate whether internet-facing VPN endpoints were included in your active attack surface inventory (CIS 1.1). Establish a process to monitor Fortinet PSIRT and CISA KEV for future advisories related to this event; subscribe to Fortinet's security advisory feed.

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 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), 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 vulnerability management platform: create a cron job or scheduled task that polls the Fortinet PSIRT RSS feed (https://www.fortinet.com/support/psirt — search-retrieved, recommend human validation) and CISA KEV JSON feed (https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json — search-retrieved, recommend human validation) daily, comparing against your confirmed FortiOS version string. For AC-7 gap analysis on FortiGate, check 'config user setting / get' for 'auth-lockout-threshold' and 'auth-lockout-duration' — the reported 1.16 billion brute-force attempts indicate these were either absent or set too permissively across the exposed population. Document findings in a lessons-learned report referencing the specific FortiBleed dataset and timeline for future audit evidence.

Evidence: For post-incident review, preserve and archive: (1) all FortiGate authentication logs from the full incident window showing the brute-force attempt volume and successful authentications — this is the primary evidence base for the lessons-learned report and any regulatory breach notification assessment; (2) a point-in-time export of the CISA KEV catalog entry if one is published for this event, dated and versioned; (3) the full AD account audit trail showing

scope of lateral movement — accounts touched, privileges escalated, time range — to accurately characterize blast radius for leadership reporting and any required breach notification analysis; (4) Fortinet PSIRT advisory if subsequently published, cross-referenced against the FortiOS versions in your environment at time of compromise.

Detection Guidance

Search VPN authentication logs for any source IP generating more than a defined threshold of failed authentication attempts (NIST AU-6, CIS 8.2) followed by a successful login; this pattern is consistent with T1110.001, T1110.002, T1110.003. Correlate successful FortiGate VPN authentications against Active Directory logon events (event IDs 4624, 4648) from the same timeframe to identify post-VPN lateral movement (T1021.002, T1078.002). Look for T1552.001 indicators: new processes querying credential stores, unexpected access to LSASS, or tools consistent with T1003 (credential dumping) on domain controllers or member servers. Flag any FortiGate management interface authentication attempts from external IPs. Because the initial extraction vector is unconfirmed, behavioral detection of unusual authentication volume, off-hours VPN sessions, new admin accounts, and unexpected SMB lateral movement is the most reliable signal. No confirmed IOC hashes or IP lists are available from authoritative sources at time of writing; treat any third-party IOC lists with caution until Fortinet PSIRT or CISA publish confirmed indicators.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`no confirmed IOCs available`	No authoritative IOC list (IP addresses, hashes, domains) has been published by Fortinet PSIRT or CISA as of source data collection. Third-party IOC lists exist but are unverified at this tier. Monitor Fortinet PSIRT and CISA for confirmed indicators.	LOW

Framework Mappings

MITRE-ATTACK

- **T1078.002** — Domain Accounts
- **T1110.003** — Password Spraying
- **T1590** — Gather Victim Network Information
- **T1110.002** — Password Cracking
- **T1083** — File and Directory Discovery
- **T1110.001** — Password Guessing
- **T1133** — External Remote Services
- **T1021.002** — SMB/Windows Admin Shares
- **T1552.001** — Credentials In Files
- **T1003** — OS Credential Dumping

- **T1005** — Data from Local System
- **T1078** — Valid 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-6** — Least Privilege
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **AT-2** — Literacy Training and Awareness
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

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

HIPAA-SECURITY

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

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
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078.002	Domain Accounts	Defense-Evasion
T1110.003	Password Spraying	Credential-Access
T1590	Gather Victim Network Information	Reconnaissance
T1110.002	Password Cracking	Credential-Access
T1083	File and Directory Discovery	Discovery
T1110.001	Password Guessing	Credential-Access
T1133	External Remote Services	Persistence
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1552.001	Credentials In Files	Credential-Access
T1003	OS Credential Dumping	Credential-Access
T1005	Data from Local System	Collection
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/fortibleed-leak-expo...	T3
Unable to access SQL Server Service via FortiClient SSL ...	https://www.reddit.com/r/fortinet/comments/tlzb6w/unable_to_access_...	T3
Microsoft SQL Server | FortiSIEM 7.5.1	https://docs.fortinet.com/document/fortisiem/7.5.1/external-systems...	T3
Fortinet Patches High-Severity Vulnerabilities	https://www.securityweek.com/fortinet-patches-high-severity-vulnera...	T3
CVE-2022-42475: Fortinet FortiOS SSL-VPN RCE ...	https://www.sentinelone.com/vulnerability-database/cve-2022-42475/	T3

Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-17 18:49 UTC by TJS Security Command Center