zensec

INCIDENT INTELLIGENCE BRIEFING : 17 JUNE 2026

FortiBleed: Mass Credential Exposure

73,932 compromised Fortinet firewall URLs across 194 countries : Russian-speaking threat actors conducting industrial-scale credential harvesting operation

EXECUTIVE SUMMARY

A coordinated credential-harvesting campaign dubbed "FortiBleed" has affected 73,932 Fortinet firewall URLs across 194 countries, impacting 21,632 unique domains. If your organisation operates Fortinet FortiGate devices, immediate verification and remediation are recommended.

Security researcher Volodymyr "Bob" Diachenko identified an exposed server operated by a Russian-speaking threat actor group. The operation executed 1.16 billion credential attempts against 320,777 FortiGate targets plus 2.1 billion attempts against 163,650 MSSQL servers: representing approximately 50% of all internet-facing Fortinet devices.

Affected organisations include major enterprises across technology, professional services, and telecommunications. Hudson Rock operates a free verification portal allowing organisations to confirm exposure status and take appropriate action.

BY THE NUMBERS

73,932
COMPROMISED FIREWALL URLS

194
COUNTRIES AFFECTED

1.16B
CREDENTIAL ATTEMPTS EXECUTED

50%
OF ALL FORTINET DEVICES

CRITICAL FINDINGS

- **Modern password policies insufficient :** complex 20-character passwords successfully compromised when credentials exist in infostealer databases harvested at endpoint level
- **SSL VPN authentication vulnerable:** authentication hashes intercepted and cracked offline using industrial-scale GPU infrastructure (45-GPU cluster via Hashtopolis)
- **Rapid lateral movement observed :** attackers pivot to internal Active Directory within 48 hours of perimeter breach, establishing persistent access beyond edge devices
- **Verified impact on critical infrastructure :** confirmed incidents include defense sector organisations with sensitive data holdings

RECOMMENDED IMMEDIATE ACTIONS

- Verify exposure status via Hudson Rock portal (hudsonrock.com/fortinet): free service confirms if your domain appears in the dataset
- Rotate all Fortinet VPN and administrative credentials as precautionary measure : prioritise accounts with elevated privileges
- Deploy MFA across all external-facing authentication points (certificate-based or hardware token recommended for high-value accounts, not SMS)
- Review authentication logs for anomalous activity patterns: focus on unusual geographic access, off-hours sessions, or unexpected privilege escalations
- Restrict administrative interface exposure to internal networks : apply access control policies limiting management plane to trusted source IPs
- Commission Active Directory audit : validate no unauthorised accounts, lateral movement indicators, or policy modifications in recent 90-day window
- Brief cyber insurance carrier on exposure assessment and document remediation timeline for compliance purposes

Incident Intelligence Briefing

zensec

ATTACK METHODOLOGY & ATTRIBUTION

Russian-Speaking Multi-Operator Group

Coordinated campaign by Russian-speaking threat actors using automated tooling to scan internet for exposed Fortinet FortiGate Management Interfaces left accessible to public.

Infostealer-Harvested Credentials

Attackers tested vast repositories of historical credential leaks harvested by infostealer malware against exposed Fortinet instances. Complex passwords offered no protection : if stolen at endpoint before encryption, no amount of complexity saves them.

SSL VPN Hash Interception & GPU Cracking

Attackers actively intercept SSL VPN authentication hashes and crack them offline using dedicated 45-GPU cluster managed via Hashtopolis. Even encrypted credentials are vulnerable when hashes can be captured and brute-forced at industrial scale.

Active Directory Pivot & Persistence

Once initial foothold established, attackers pivot directly into internal Active Directory environments within 48 hours, enabling deep persistent network access that survives routine security checks and password resets on edge devices.

BUSINESS IMPACT & LEGAL CONSIDERATIONS

This incident constitutes a reportable data exposure event. Organisations appearing in the FortiBleed dataset hold compromised credentials that may require GDPR breach notification assessment. Consult legal counsel regarding ICO notification obligations within the 72-hour statutory window.

The campaign demonstrates the limitations of password-based perimeter security when credentials are harvested at the endpoint before encryption. Complex password policies remain necessary but insufficient: defence requires layered controls including MFA, network segmentation, and continuous monitoring.

Cyber insurance carriers typically require prompt notification of potential exposure events. Timely remediation and documentation of response actions support policy compliance and demonstrate reasonable security governance to stakeholders.

REFERENCES & INTELLIGENCE SOURCES

- Hudson Rock (17 June 2026): FortiBleed - 73,932+ Compromised Fortinet Firewalls (Free Verification Portal)
- Cyber Security News (17 June 2026): FortiBleed - 70,000+ Fortinet Firewalls Compromised in Massive Exploitation Attack
- Volodymyr "Bob" Diachenko (LinkedIn, 17 June 2026): Original FortiBleed Discovery
- The Hacker News (17 June 2026): Attackers Exploit Three Fortinet FortiSandbox Flaws

RECOMMENDED FOLLOW-UP ACTIONS

- Apply latest FortiOS security updates: prioritise internet-facing SSL VPN gateways and management interfaces in patching schedule
- Enhance network segmentation to limit lateral movement pathways from perimeter devices to internal infrastructure
- Deploy or tune SIEM capabilities: focus on Active Directory enumeration, unusual SMB/RDP patterns, and data staging activities
- Review VPN account provisioning : validate all accounts created in past 180 days correspond to legitimate business requirements

ZENSEC RESPONSE SERVICES

- 24/7 Incident Response Retainer: immediate breach triage, forensic analysis, and containment
- Digital Forensics & Incident Response (DFIR): CREST-certified investigation and evidence collection, NCSC Assured Cyber Incident Response
- Ransomware Data Recovery: secure backup restoration and encrypted data recovery where possible
- vCISO Managed Service: strategic incident management, board reporting, and regulatory liaison
- Post-Incident Security Hardening: architecture review, MFA deployment, and continuous monitoring

24/7 EMERGENCY RESPONSE LINE

zensec.co.uk

0333 091 7040 · Immediate Assistance

contact@zensec.co.uk