ADVISORY ISSUED: 'FortiBleed' Credential Exposure Affecting 73,000+ Fortinet Firewall Devices

'FortiBleed' is a critical database exposure containing active credentials affecting more than 73,000 Fortinet devices, from firewalls to VPN Gateways. There are reports from around the globe that these credentials are being actively exploited in both public and private sector organizations.

Arete is issuing guidance for our partners and clients to assist in mitigating risk, detecting potential unauthorized access, and preparing for the increasing number of threat actors attempting to utilize this exposure to gain initial access.

External Information About FortiBleed:

CISA Urges Hardening Fortinet Devices After Reports of Credential Exposure | CISA

FortiBleed 2026: 86,644 Fortinet Firewalls Compromised — Active Leak

FortiBleed - 70,000+ Fortinet Firewalls Compromised in Massive Exploitation Attack

Important Considerations:

1. This leak is not the result of software-based CVEs or access control flaws. The affected database contains verified and functional credentials for thousands of devices around the world, regardless of firmware patching level.

2. Many Fortinet devices use external identity providers to manage account access and VPN sign-in. This means that the credentials involved in this database may affect more than just the Fortinet devices themselves—they could also provide access to external services, including email, cloud hosting providers, business-critical SaaS applications, and more.

3. There is no singular 'fix' to mitigate this database exposure. It is important to work with your security team, incident response provider, and other stakeholders to review environments holistically and monitor for signs of potentially unauthorized activity.

Immediate Containment Actions:

Arete recommends the following steps to assist with evaluating ongoing exposure and mitigating potential unauthorized access related to 'FortiBleed':

1. End all administrative user sessions in the firewall(s).
2. End all SSL VPN sessions in the firewall(s) and, ideally, temporarily disable SSL VPN services.
3. Revoke any active tokens/sessions on local devices or identity providers.
    a. This may include connected services like M365, Google, etc., if they use Active Directory or Entra as an identity provider. This is a credential compromise-based alert, which means unauthorized access to other services related to those credentials could have already occurred.
4. Create a configuration backup of the firewall(s) and store securely.
5. Disable firewall management interfaces (HTTP/S, SSH, etc.) on any external, public, or unnecessary interfaces to ensure the firewall is only accessible via approved and secured networks and locations.
    a. Consider adding IP-based policies to restrict access to known internal addresses or VPN addresses of approved management users.
6. Export and retain any available logging for administrative, traffic, VPN, and authentication activity that has taken place on the firewall(s).

Credential Compromise Mitigation Actions:

1. Reset all firewall administrator passwords (Local and LDAP/AD/etc).
    a. Verify that all administrative users are recognized and require that level of access.
    b. Remove unrecognized users and those who no longer require that access level.
2. Reset all SSL VPN user passwords.
    a. Local Accounts should be reset on each firewall device. Any local FortiTokens/MFA should also be reset.
    b. LDAP/RADIUS/etc. integrated accounts should have password resets triggered immediately on the respective identity source. This should also

include an MFA reset and existing session closure on the respective platform.

3. Disable or rename any default-named local accounts on the firewall to something unique.

4. Rotate service account password(s) used for things like LDAP/RADIUS/AD and ensure the account has the lowest rights required on the IdP side to mitigate the risk of compromise.

5. Ensure all firewalls in the environment utilize unique local credentials and do not share common login/administrative information.

6. Reset MyFortinet and Support Portal cloud account passwords to ensure configuration backups and management access remain secure.

    a. Verify that all users in cloud services are recognized and still require platform access.

Additional Hardening Actions:

1. Enforce Multi-Factor Authentication on all VPN and administrative accounts.

    a. Wherever possible, utilize Phishing-Resistant MFA

2. Enforce a strong password policy (locally and/or via the configured IdP) to ensure new user passwords meet stringent security requirements and mitigate reuse of old credentials.

3. Review external services available on the firewall (web servers, mail, etc.), verify a continued need for access, and ensure that least-access design is factored into the NAT/firewall rules and their application.

    a. Disable any unused services or rules.

    b. Disable any unused or non-required firewall services that face "public" interfaces.

4. Patch the Fortinet firewall(s) to their latest license and support level, following their upgrade path tool: https://docs.fortinet.com/upgrade-tool/fortigate%C2%A0and

    a. Configuration backups should be taken at each step for preservation and fallback as needed.

b. After each upgrade step, local account passwords will need to be cycled for each release in the upgrade chain to mitigate other past Fortinet CVEs.

c. Firmware should only be obtained from Fortinet directly, utilizing existing support portal access.

d. Ensure firewall(s) utilize PBKDF2 hashing for accounts, following Fortinet's guidance: Technical Tip: Enforcing PBKDF2 as hash function for administrator accounts in FortiOS v7.2.11 and later | Community

Detection and Investigation Actions:

1. Engage security stakeholders for assistance reviewing the environment for signs of compromise or unauthorized access.

2. Review firewall, VPN, and authentication logs for unknown/unrecognized activity or accounts, unusual behavior or access times/lengths, or the creation of new accounts in the environment (especially those given elevated rights shortly after).

3. Review Active Directory logging, accounts, and access levels in the environment, especially if any credentials are tied to Fortinet administration or VPN access in any way. This could help identify signs of persistent access or additional response actions needed.

4. Rotate all privileged and service account passwords in the environment as a precaution to mitigate potential compromise or persistent access.

5. Verify that EDR/ RMM/endpoint security products are actively deployed across 100% of the landscape. If any gaps are identified, they should be remediated immediately.

6. Look for unauthorized or unrecognized policy changes (AD, Entra, Intune, etc.) in the environment and investigate any actions that flag.

Additional Event Context

The credentials in the campaign resulted from an aggressive, large-scale credential-harvesting and valid account abuse campaign against Fortinet FortiGate firewalls and SSL-VPN gateways. The campaign relied on automated password spraying and configuration exfiltration rather than vulnerability exploitation. In some cases, the threat actors exfiltrated configuration files, which they were able to crack if organizations did not have administrators re-authenticate after Fortinet implemented a firmware update in early 2025 that hardened the cryptography protecting administrator credentials.

Following initial access, operators deployed packet-sniffing capabilities and established external listening posts to receive harvested credentials and session data in near real time. This means impacted organizations may have credential exposure well beyond their Fortinet device.

The scale of exposure and attack activity was significant and globally distributed. Analysis estimated approximately 1.16 billion credential attempts were executed against more than 320,000 FortiGate devices. In parallel, over 2.1 billion brute-force attempts were directed at more than 160,000 MSSQL database installations, suggesting coordinated targeting beyond edge appliances and into internal data services. At peak exposure, more than 73,000 unique FortiGate units were identified as directly accessible across 194 nations. The threat actor explicitly categorized exposed organizations by industry and revenue, indicative of staging for future credential sale or targeted intrusions.

How Arete Can Help

Arete is fully prepared to utilize our extensive experience with detection, threat hunting, and attack surface review to look for indications of unauthorized activity related to this database exposure. Should any issues be identified or require additional investigation, Arete has teams of investigators ready to engage with our clients and partners to conduct a full environment review, safely implement recommended mitigation steps, and provide any additional response services that may be required based on findings by our team of experts who have years of experience in investigations and forensic review.

Contact Us

Email: arete911@areteir.com
Phone: +1-866-210-0955