# TECHNICAL ADVISORY

## FortiBleed Campaign Targeting Fortinet Firewalls and VPN Gateways

### 1.0. BACKGROUND

A large-scale cybercrime campaign, known as "FortiBleed," is actively targeting Fortinet FortiGate firewalls and SSL VPN Gateways. The campaign leverages credential harvesting and password-spraying techniques to gain unauthorised access to exposed systems.

The campaign does not rely on a newly discovered vulnerability but instead exploits weak credential practices, including password reuse and lack of multi-factor authentication (MFA).

### 2.0. THREAT SUMMARY

Threat actors are conducting automated scanning of internet-facing Fortinet devices and testing them against large datasets of previously leaked credentials. Valid credentials are catalogued and reused, enabling attackers to access systems at scale across multiple sectors.

Once access is obtained, attackers may use the compromised devices to monitor network traffic, capture authentication data, and establish persistent access. This can lead to lateral movement, privilege escalation, and compromise of other internal systems, including Active Directory environments.

### 3.0. RISK EXPOSURE

Organisations may be at increased risk if:

- Administrative or VPN interfaces are publicly accessible
- Passwords are reused, weak, or not regularly rotated
- MFA is not enforced for remote or administrative access
- Administrative access is not restricted to trusted IP sources

### 4.0. INDICATORS OF COMPROMISE

Organisations should review logs and investigate the following:

- Login activity from unusual locations or times
- Repeated failed logins followed by successful access
- Unknown or unauthorised administrator accounts
- Unexpected configuration changes on firewalls
- Irregular VPN usage, including concurrent or anomalous sessions
- Network connections to suspicious or unfamiliar IP addresses

The presence of the above indicators may suggest attempted or successful compromise and should trigger immediate response actions.

Organisations can perform an initial exposure check using: https://socradar.io/free-tools/fortibleed.

## 5.0. RECOMMENDATIONS

### 5.1. Immediate Measures

- Rotate all administrative and VPN credentials
- Enforce multi-factor authentication (MFA)
- Enforce the use of strong, unique passwords

### 5.2. Other Measures

- Restrict access to administrative interfaces to trusted IP addresses or internal networks
- Disable unnecessary services, including unsecured management interfaces, to reduce exposure
- Continuously monitor firewall, VPN, and authentication logs to support investigation and incident response
- Implement network segmentation and least privilege access controls to limit lateral movement in the event of a breach
- Update all Fortinet devices with the latest firmware and configurations in accordance with the vendor's recommendations

The CSA maintains a 24-hour Cybersecurity/Cybercrime Incident Reporting Point of Contact (PoC). Call or Text – 292, WhatsApp – 0501603111, or Email – report@csa.gov.gh for assistance related to this advisory.

**Issued by the Cyber Security Authority**
**June 19, 2026**
**Ref: CERT/TA/2026-06/01**