GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

24 June 2026

Advisory 149: FortiBleed – Widespread Credential Exposure Targeting Fortinet Firewalls and SSL VPN Gateways

Release Date: 22nd June 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CERT Vanuatu advises on FortiBleed, a large-scale credential exposure campaign targeting Fortinet FortiGate Firewalls and SSL VPN gateways**.** Unlike a traditional software vulnerability, FortiBleed is a credential compromise campaign where attackers leverage leaked, stolen, or exposed administrator and VPN credentials to gain unauthorized access to Fortinet devices.

What are the systems affected?

The campaign affects organizations using:

- FortiGate Firewalls
- FortiGate SSL VPN Gateways
- FortiOS Management Interfaces
- Internet-facing Fortinet Appliances

Organizations are particularly at risk if they:

- Expose firewall management interfaces to the Internet
- Use outdated FortiOS firmware
- Have administrator or VPN credentials that have been leaked or reused
- Do not enforce Multi-Factor Authentication (MFA)
- Store administrator credentials using legacy password hashing methods instead of **PBKDF2**

What does this mean?

Step 1 – Credential Acquisition

Attackers obtain valid credentials through:

- Previous data breaches
- Infostealer malware infections
- Credential stuffing attacks

Step 2 – Authentication Using Legitimate Credentials

Attackers authenticate to:

- FortiGate administrative portals
- SSL VPN gateways
- Remote management interfaces

Because valid credentials are used, login attempts often appear legitimate and bypass many traditional security controls.

Step 3 – Privilege Abuse

After successful authentication, attackers may:

- Create new administrator accounts
- Reset passwords
- Disable security logging
- Modify firewall rules

Step 4 – Internal Network Compromise

Compromised Fortinet devices become an entry point into the organization's internal network.

Attackers may then:

- Move laterally across systems
- Harvest additional credentials

4. Potential Impact

Successful exploitation may allow attackers to:

- Gain full administrative control of Fortinet appliances
- Access internal enterprise networks
- Modify firewall and VPN configurations
- Disable security monitoring

Mitigation process

1. Terminate Active Sessions and Rotate Credentials (Critical)

Immediately:

- Terminate all active SSL VPN sessions
- Terminate all administrator sessions
- Reset all administrator passwords
- Reset all VPN user passwords
- Rotate service account credentials

Implement strong password policies and prohibit password reuse.

2. Apply the Latest Fortinet Firmware Updates

- Upgrade FortiOS to the latest supported version.
- Apply all Fortinet security updates and hotfixes.
- Remove unsupported firmware versions from production environments.

3. Enforce Secure Credential Storage

Verify that administrator credentials are stored using:

Password-Based Key Derivation Function 2 (PBKDF2)

Organizations should:

- Upgrade to FortiOS versions supporting PBKDF2
- Require all administrator accounts to log in after upgrading
- Ensure legacy password hashes are replaced with PBKDF2 hashes

This significantly improves resistance against offline password-cracking attacks.

4. Enable Phishing-Resistant Multi-Factor Authentication (MFA)

Require MFA for:

- Firewall administrator accounts
- SSL VPN users
- Remote management interfaces

- External administrative access

Hardware security keys or phishing-resistant authentication methods are strongly recommended.

Reference

1. https://www.cisa.gov/news-events/alerts/2026/06/18/cisa-urges-hardening-fortinet-devices-after-reports-credential-exposure
2. https://www.cyber.gov.au/about-us/view-all-content/Reported-widespread-credential-exposure-affecting-Fortinet-Firewalls-and-VPN-Gateways
3. https://www.fortinet.com/blog/psirt-blogs/analysis-of-reported-credential-compromise-of-fortigate-devices

.