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

19 June 2026

Advisory 147: Widespread credential Exposure Affecting Fortinet Firewalls and VPN Gateways

Release Date: 18th 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 a widespread malicious campaign targeting Fortinet Firewalls and VPN gateways. Unlike a single software vulnerability, this campaign primarily involves the compromise, theft, and abuse of administrative and VPN credentials, enabling attackers to gain unauthorized access to Fortinet devices and connected networks.

Attackers are leveraging exposed, weak, reused, or previously compromised credentials to authenticate to Fortinet infrastructure and potentially bypass security controls without exploiting a software vulnerability.

What are the systems affected?

The campaign affects organizations using:

- FortiGate firewalls
- FortiGate SSL VPN services
- Fortinet administrative management interfaces
- Internet-facing Fortinet security appliances
- Organizations using outdated or unpatched Fortinet firmware

Systems at highest risk include:

- Firewalls with exposed management interfaces
- VPN gateways accessible from the internet
- Devices using weak, reused, or compromised credentials
- Systems not protected by Multi-Factor Authentication (MFA)

What does this mean?

Typical exploitation flow:

1. Credential Acquisition

Attackers obtain credentials through:

- Previous data breaches
- Credential stuffing attacks
- Phishing campaigns
- Malware infections
- Brute-force attacks against exposed login portals

2. Authentication to Fortinet Devices

Using valid credentials, attackers log into:

- Administrative web interfaces
- SSL VPN portals
- Remote management services

Because the credentials are legitimate, the activity may initially appear normal.

3. Establishing Access

Once authenticated, attackers may:

- Create new administrator accounts
- Modify firewall rules
- Disable security controls
- Access internal networks

- Deploy persistence mechanisms

4. Lateral Movement

Attackers can then:

- Access internal servers
- Harvest additional credentials
- Move across the network
- Target critical business systems

Mitigation process

1. Rotate All Credentials Immediately (Critical)

Rotate:

- Firewall administrator passwords
- VPN user passwords
- Service accounts
- Shared administrative accounts

Assume exposed credentials may already be compromised.

2. Enable Multi-Factor Authentication (MFA)

Enforce MFA for:

- Administrative access
- SSL VPN access
- Remote management interfaces

This significantly reduces the effectiveness of stolen credentials.

3. Patch and Update Fortinet Devices

- Upgrade to the latest Fortinet firmware versions
- Apply all vendor security advisories and hotfixes
- Remove unsupported firmware versions from production

4. Restrict Management Interface Exposure

- Do not expose management interfaces directly to the internet
- Restrict access through:
    - VPN
    - Dedicated management networks
    - IP allowlisting

- Bastion hosts

Reference

1. https://www.cyber.gov.au/about-us/view-all-content/Reported-widespread-credential-exposure-affecting-Fortinet-Firewalls-and-VPN-Gateways
2. https://www.ncsc.gov.uk/news/advice-following-global-targeting-of-fortinet-firewalls-and-vpn-gateways

.