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

21 May 2026

Advisory 142: Fortinet FortiAuthenticator Vulnerability

Release Date: 12th May 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?

CVE-2026-44277 is a critical vulnerability (CVSS 9.8) affecting Fortinet FortiAuthenticator. The flaw is classified as an improper access control vulnerability (CWE-284).

What are the systems affected?

The following versions of Fortinet FortiAuthenticator are affected:

- FortiAuthenticator **8.0.0** and **8.0.2**
- FortiAuthenticator **6.6.0 through 6.6.8**
- FortiAuthenticator **6.5.0 through 6.5.6**
- FortiAuthenticator **6.4.0 through 6.4.10**

What does this mean?

The vulnerability is **network exploitable** and may be exploited **without authentication**.

Typical exploitation flow:

1. **Target discovery**
    - Attackers identify internet-facing FortiAuthenticator appliances.
2. **Crafted request delivery**
    - Malicious HTTP/HTTPS requests are sent to vulnerable services or management interfaces.
3. **Access control bypass**
    - The appliance improperly validates access permissions.
4. **Unauthorized command or code execution**
    - The attacker executes commands or interacts with privileged functionality.
5. **Post-compromise activity**
    - Attackers may:
        - Steal authentication data
        - Manipulate MFA workflows
        - Create unauthorized accounts
        - Pivot into internal enterprise systems

Mitigation process

CERTVU recommends the following;

- upgrading to patched versions:

    - 6.5.7 or later
    - 6.6.9 or later
    - 8.0.3 or later

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://nvd.nist.gov/vuln/detail/CVE-2026-44277
3. https://fortiguard.fortinet.com/psirt/FG-IR-26-128

.