

**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



**GOVERNEMENT 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 151: Ubiquiti UniFi OS Path Traversal Vulnerability.

Release Date: 23rd 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?

CVE-2026-34909 is a critical Path Traversal vulnerability affecting Ubiquiti UniFi OS devices. The flaw allows a malicious actor with network access to access files on the underlying operating system that should not be accessible through the application. These files may then be manipulated or leveraged to gain access to an underlying system account.

What are the systems affected?

The vulnerability affects multiple **Ubiquiti UniFi OS** products, including:

- UniFi OS Server - 5.0.8 or later
- Express – 4.0.14 or later
- UDM – 5.1.12 or later
- UDM-Pro – 5.1.12 or later
- UDM-SE – 5.1.12 or later
- UDM-Pro-Max – 5.1.12 or later

- UDM-Beast – 5.1.11 or later
- EFG – 5.1.12 or later
- UDW – 5.1.12 or later
- UDR – 5.1.12 or later
- UDR7 – 5.1.12 or later
- UDR-5G – 5.1.12 or later
- Express 7 – 5.1.12 or later

What does this mean?

Typical Attack Process

Step 1 – Identify Accessible Devices

Attackers identify UniFi OS management interfaces that are reachable from internal or external networks.

Step 2 – Exploit Path Traversal

By submitting specially crafted requests containing manipulated file paths (for example, directory traversal sequences), an attacker may bypass intended directory restrictions and access sensitive files on the underlying operating system.

The vulnerability exists because the application does not properly validate or sanitize file paths before processing them.

Step 3 – Access Sensitive Files

Successful exploitation may expose files containing:

- System configuration data
- Authentication tokens
- Application secrets
- Service credentials
- Account-related information

These files may then be manipulated or used to compromise an underlying system account.

Mitigation process

CERTVU recommends the following:

1. Update UniFi OS Immediately (Critical)

Upgrade affected devices to the latest patched versions:

- UniFi OS Server 5.0.8 or later
- Express 4.0.14 or later
- UDM/UDM-Pro/UDM-SE/UDM-Pro-Max/UDR/UDW/EFG/Express 7 5.1.12 or later

- UDM-Beast 5.1.11 or later

2. Restrict Management Interface Access

- Do not expose UniFi OS management interfaces directly to the Internet.
- Restrict access to:
 - Dedicated management VLANs
 - Trusted internal networks
 - VPN connections
 - IP allowlists

This significantly reduces the attack surface.

Reference

1. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
2. <https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b>
3. <https://www.cve.org/CVERecord?id=CVE-2026-34909>