

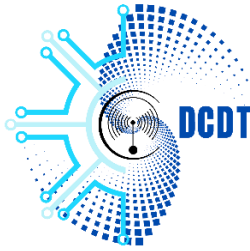
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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 150: Ubiquiti UniFi OS Improper Access Control 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-2026-34908 is a critical Improper Access Control vulnerability affecting Ubiquiti UniFi OS devices. The vulnerability allows an unauthenticated attacker with network access to make unauthorized changes to the system, potentially resulting in complete compromise of the device and the networks it manages.

What are the systems affected?

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

- UniFi OS Server
- UniFi Dream Machine (UDM)
- UniFi Dream Machine Pro (UDM-Pro)
- UniFi Dream Machine SE (UDM-SE)
- UniFi Dream Router (UDR)
- UniFi Express

- UniFi Network Video Recorders (UNVR/UNVR-Pro)
- UniFi Cloud Gateways and other UniFi OS-based consoles running vulnerable firmware versions.

What does this mean?

Typical Attack Process

1. **Identify Accessible Devices**
 - Attackers locate UniFi OS management interfaces that are reachable over the network.
2. **Send Crafted Requests**
 - Specially crafted requests are sent to management or API endpoints that do not properly enforce authorization.
3. **Bypass Access Controls**
 - Due to improper access validation, the device processes privileged requests without requiring valid administrator credentials.
4. **Modify System Configuration**
 - Attackers can perform unauthorized administrative actions such as:
 - Creating administrator accounts
 - Modifying firewall rules
 - Changing network and VPN settings
 - Altering routing or DNS configurations
 - Disabling security features

Mitigation process

CERTVU recommends the following:

1. Update UniFi OS Immediately (Critical)

Upgrade all affected UniFi OS devices to the latest firmware versions released by Ubiquiti that address the vulnerability.

2. Restrict Management Interface Access

- Do not expose UniFi OS management interfaces directly to the Internet.
- Restrict access to trusted internal networks or management VLANs.
- Use VPN access for remote administration.
- Implement IP allowlists where possible.

3. Monitor for Unauthorized Changes

Review audit logs for:

- Unexpected administrator account creation
- Firewall or routing configuration changes
- DNS or VPN modifications
- Administrative requests from unfamiliar IP addresses

Reference

1. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
2. <https://www.cve.org/CVERecord?id=CVE-2026-34908>
3. <https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b>