مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Ubiquiti UniFi OS Devices

Tracking #:432319032

Date:25-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Ubiquiti has released Security Advisory Bulletin addressing five critical vulnerabilities affecting multiple UniFi OS devices and UniFi OS Server deployments.

TECHNICAL DETAILS:

Ubiquiti has released Security Advisory Bulletin addressing five critical vulnerabilities affecting multiple UniFi OS devices and UniFi OS Server deployments. The vulnerabilities include Improper Access Control, Command Injection, and Path Traversal flaws that could allow remote attackers to gain unauthorized access, execute commands, manipulate system configurations, and access sensitive files.
Several of the disclosed vulnerabilities carry a maximum CVSS score of 10.0 Critical, indicating severe risk to affected environments. Successful exploitation could lead to full system compromise, unauthorized administrative actions, credential theft, and exposure of sensitive information.
Organizations using affected UniFi products should prioritize immediate patching and review device exposure to untrusted networks.

Vulnerability Details

1. Command Injection Vulnerability

CVE Information

- CVE ID: CVE-2026-33000
- CVSS Score: 9.1 Critical

Fixed Version

- UniFi OS Server Version 5.0.8 or later

2. Improper Access Control Vulnerability

CVE Information

- CVE ID: CVE-2026-34908
- CVSS Score: 10.0 Critical

Fixed Versions

- Most affected devices: Version 5.1.12 or later
- UniFi OS Server: Version 5.0.8 or later
- UNAS devices: Version 5.1.10 or later
- UDM-Beast: Version 5.1.11 or later

3. Path Traversal Vulnerability

CVE Information

- CVE ID: CVE-2026-34909
- CVSS Score: 10.0 Critical

Fixed Versions

- Most affected devices: Version 5.1.12 or later
- Express: Version 4.0.14 or later
- UniFi OS Server: Version 5.0.8 or later

4. Remote Command Injection Vulnerability

CVE Information

- CVE ID: CVE-2026-34910
- CVSS Score: 10.0 Critical

Fixed Versions

- Most affected devices: Version 5.1.12 or later
- UniFi OS Server: Version 5.0.8 or later

5. Path Traversal Information Disclosure Vulnerability

CVE Information

- CVE ID: CVE-2026-34911
- CVSS Score: 7.7 High

Fixed Versions

- Most affected devices: Version 5.1.12 or later
- UniFi OS Server: Version 5.0.8 or later

RECOMMENDATIONS:

- Immediately update all affected UniFi OS devices to the latest patched versions.
- Prioritize internet-exposed UniFi management interfaces and controllers.
- Disable external administrative access where not required.
- Review firewall rules restricting access to UniFi management services.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b