



# Critical Vulnerability in Ubiquiti UniFi OS Devices

25 May 2026

**CONFIDENTIAL:** The content of this document is intended solely for use by the natural or legal person to whom it is addressed. If you gain access to this document by mistake, you should be aware that any forwarding, copying or disclosure of its content to any other person is strictly prohibited, and you must inform the sender immediately.

## EXECUTIVE SUMMARY:

The Digital Security Authority (DSA) wants to bring to your attention 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.

### Vulnerabilities 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:

The Digital Security Authority (DSA) recommends applying the mitigation or workaround provided by Ubiquiti.

- 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.

Please ensure to distribute this information among your subsidiaries and partners and provide us with any pertinent information or findings you may have (such as Indicators of Compromise, Tactics, Techniques, and Procedures, etc.).

The Digital Security Authority (DSA) extends its appreciation for the continued collaboration.

## REFERENCES:

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

## DISCLAIMER:

The information presented in this report is based on available data up to the 25<sup>th</sup> of May 2026.

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.