# Ubiquiti UniFi OS Multiple Vulnerabilities

**Severity Level:** Critical

## Components Affected

- Ubiquiti UniFi OS
- UniFi Gateways
- UniFi Routers
- UniFi Network Video Recorders (NVRs)
- UniFi Controllers and appliances running affected UniFi OS versions

## Overview

Multiple vulnerabilities have been identified in Ubiquiti UniFi OS products. An attacker with network access may exploit these vulnerabilities to read files, execute arbitrary commands, and gain complete control of affected devices.

## Description

Multiple critical vulnerabilities have been identified in Ubiquiti UniFi OS, affecting UniFi Gateways, Routers, Network Video Recorders (NVRs), and Controller appliances. The vulnerabilities include improper access control, path traversal, and information disclosure flaws that could be exploited by an attacker with network access to the affected devices.

Successful exploitation of these vulnerabilities could allow an attacker to bypass security restrictions, read sensitive files, execute arbitrary commands, and perform unauthorized administrative actions on vulnerable systems. In certain scenarios, an attacker may be able to gain full control of the affected device, modify configurations, create unauthorized accounts, deploy malicious payloads, or use compromised devices as a pivot point to move laterally within the network.

Ubiquiti has confirmed that these vulnerabilities are being actively exploited in the wild. Organizations using affected UniFi OS products are strongly advised to apply the latest security updates and review their environments for indicators of compromise.

## Impact

- Arbitrary Command Execution
- Unauthorized File Access
- Complete Device Compromise
- Information Disclosure
- Potential Network Lateral Movement
- Service Disruption and Administrative Takeover

## Solution/ Workarounds

- Upgrade UniFi OS to the latest vendor-recommended version.
- Apply all security patches released by Ubiquiti.
- Restrict management access to trusted networks only.
- Monitor devices for suspicious administrative activity.
- Review logs and indicators of compromise on affected systems.
- Change administrative credentials if compromise is suspected.

## Reference

- https://cybernews.com/security/critical-ubiquiti-unifios-bugs-exploited-by-hackers
- https://www.securityweek.com/critical-ubiquiti-vulnerabilities-in-attackers-crosshairs

## Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.