Ubiquiti Addresses Multiple Vulnerabilities Across UniFi Products

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

Ubiquiti released security updates for 25 vulnerabilities affecting multiple UniFi products, including UniFi OS, UniFi Connect, UniFi Network, UniFi Protect, UniFi Access, and UniFi Talk.

Several vulnerabilities are rated critical and could allow command injection, authentication bypass, privilege escalation, server-side request forgery (SSRF), SQL injection, or denial-of-service (DoS) attacks.

Overview

Ubiquiti released security updates for 25 vulnerabilities affecting multiple UniFi products, including UniFi OS, UniFi Connect, UniFi Network, UniFi Protect, UniFi Access, and UniFi Talk. UniFi is Ubiquiti's centralized management platform used to configure and manage enterprise networking equipment, wireless access points, gateways, switches, surveillance cameras, door access systems, VoIP communications, and other connected infrastructure. It is commonly used by businesses, managed service providers (MSPs), educational institutions, healthcare organizations, retailers, hospitality providers, and government agencies.

The vulnerabilities include:

CVE-2026-50746 (CVSS 10.0) – UniFi Connect

- An improper access control vulnerability that could allow a network-based attacker to execute arbitrary operating system commands on the host device through command injection.

CVE-2026-50747 (CVSS 9.9) – UniFi Talk

- A series of authenticated SQL injection vulnerabilities that could allow a low-privileged attacker to escalate privileges on the host device.

CVE-2026-50748 (CVSS 9.9) – UniFi Access

- An improper input validation vulnerability that could allow a low-privileged attacker to execute arbitrary operating system commands on the host device through command injection.

CVE-2026-54402 (CVSS 9.9) – UniFi OS

- An improper input validation vulnerability that could allow a low-privileged attacker to execute arbitrary operating system commands on affected UniFi OS devices.

CVE-2026-55115 (CVSS 9.9) – UniFi Protect

- A server-side request forgery (SSRF) vulnerability that could allow a low-privileged attacker to escalate privileges on the host device.

Additional High and Critical Vulnerabilities

- Ubiquiti also addressed additional vulnerabilities affecting UniFi products, including authentication bypass, privilege escalation, path traversal, denial-of-service, and improper access control vulnerabilities.

Ubiquiti has released security updates for all affected products. Organizations using affected UniFi products should apply the updates as soon as possible. At the time of publication, Ubiquiti has not reported active exploitation.

Aspire Protects

- **Patch** – See Ubiquiti's security advisory for more information.
- UniFi Connect Command Injection Vulnerability (CVE-2026-50746)
  - Upgrade UniFi Connect Application to version 3.4.20 or later.
- UniFi Talk Vulnerabilities (CVE-2026-50747, CVE-2026-55113, CVE-2026-55119)
  - Upgrade UniFi Talk Application to version 5.2.2 or later.
- UniFi Access Vulnerabilities (CVE-2026-50748, CVE-2026-54400, CVE-2026-55117)
  - Upgrade UniFi Access Application to version 4.2.29 or later.
- UniFi OS Vulnerabilities (including CVE-2026-54401, CVE-2026-54402, CVE-2026-54403, CVE-2026-54404, CVE-2026-55110, CVE-2026-55112, CVE-2026-55116)
  - Upgrade affected UniFi OS devices to version 5.1.19 or later.
- UniFi Network Vulnerabilities
  - Upgrade UniFi Network Application to version 10.4.57 or later.
- UniFi Protect Vulnerabilities
  - Upgrade UniFi Protect Application to version 7.1.83 or later.
- UniFi Protect Floodlight
  - Upgrade UniFi Protect Floodlight to version 1.13.6 or later.
- Monitor UniFi logs for unexpected authentication attempts, privilege escalation activity, configuration changes, and command execution.
- Ensure administrative accounts use strong passwords and multi-factor authentication.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – An attacker may exploit vulnerable UniFi applications or UniFi OS management interfaces exposed to the network. [CVE-2026-50746, CVE-2026-54403.

Execution

- Command and Scripting Interpreter: Unix Shell [T1059.004] – An attacker may execute arbitrary operating system commands through command injection vulnerabilities. [CVE-2026-50746, CVE-2026-50748, CVE-2026-54402]

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – An attacker may exploit vulnerabilities to obtain elevated privileges on affected UniFi devices. [CVE-2026-50747, CVE-2026-55115]

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations that use Ubiquiti UniFi products to manage enterprise networking, wireless infrastructure, surveillance systems, physical access control, or VoIP communications may be affected.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations

center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
    - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
    - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Security Advisory Bulletin 066 | Ubiquiti Community