Multiple Critical Flaws Patched in Ubiquiti UniFi OS

Jul 08, 2026

WHITE

View Alert

On July 2, 2026, Ubiquiti released critical security updates to patch seven severe vulnerabilities across its UniFi OS ecosystem, including a maximum-severity flaw CVE-2026-50746 in the UniFi Connect Application.

Additional Info

Analysis

The CVE-2026-50746 flaw allows network-based attackers to execute command injection attacks against systems that manage smart building operations, such as EV chargers and lighting.

Six additional critical flaws tracked as CVE-2026-50747, CVE-2026-50748, CVE-2026-54400, CVE-2026-54402, CVE-2026-55115, CVE-2026-55116, affect other major components, including UniFi Talk, Access, Protect, routers, gateways, and storage systems, and can be exploited via low-complexity attacks requiring zero user interaction.

While there is no current evidence that these flaws are being exploited in the wild, threat intelligence firms have identified over 100,000 internet-exposed UniFi OS instances, making them prime targets for cybercriminals and state-sponsored groups that have historically hijacked Ubiquiti hardware to build stealthy botnets.

Recommendations

- Apply the latest firmware and software updates to your UniFi routers, gateways, Protect cameras, Access systems, Talk apps, and UniFi OS Servers to patch the flaws.
- If your UniFi OS management portal is exposed to the public internet, restrict external access. Use a secure VPN or UniFi's official cloud portal to manage your network instead of leaving it directly searchable online.
- Enable automatic security updates in your UniFi OS settings so your system receives emergency patches as soon as they are released.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

<hr size=1 width="100%" align=center>

Alert Id	add40f37
Category	Vulnerability Bulletins
Tags	CVE-2026-55116, CVE-2026-55115, CVE-2026-54402, CVE-2026-54400, CVE-2026-50748, CVE-2026-50747, CVE-2026-50746, Ubiquiti

---

Sources

https://community.ui.com/releases/Security-Advisory-Bulletin-066-066/984eceb3-49c8-4227-942d-671c289b3afc
https://www.bleepingcomputer.com/news/security/ubiquiti-warns-of-new-max-severity-unifi-os-vulnerability/

Incident Date

Jun 10, 2026 (UTC)

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Please provide your feedback

Like Dislike

Download the App
Available on iOS, Android and Web

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**
Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to **toc@h-isac.org**

--
You received this message because you are subscribed to the Google Groups "TLP Green - Health-ISAC Partners" group.
To unsubscribe from this group and stop receiving emails from it, send an email to health-isac-partners+unsubscribe@h-isac.org.
To view this discussion visit https://groups.google.com/a/h-isac.org/d/msgid/health-isac-partners/0100019f41b07d31-2b0aaf42-4fa5-4864-9d64-2fbb50c123ea-000000%40email.amazonses.com.