VULNERABILITY BULLETINS

TP-Link Security Advisory Released (CVE-2025-7850 and CVE-2025-7851)

TLP:WHITE

Oct 22, 2025

On October 21, 2025, TP-Link released a security advisory concerning its Omada gateway devices to address two severe vulnerabilities, tracked as CVE-2025-7850 and CVE-2025-7851.

The first flaw allows command execution, while the second provides root shell access, posing an extreme risk of full network compromise. Immediate firmware updates are strongly recommended for all affected models to prevent full device compromise.

Health-ISAC is sharing this to increase situational awareness and encourage organizations to assess their level of risk to these vulnerabilities.

Analysis

The vulnerabilities affect the TP-Link Omada line of gateways, which function as central network components for small and medium-sized businesses. Given the gateways' role, these devices are high-value targets for threat actors. Exploitation of a vulnerable gateway device allows an attacker to compromise an organization’s network, leading

to severe consequences such as data theft, lateral movement, and persistent access.

Exploiting these flaws allows threat actors to gain total administrative and operational control of the gateway. The ability to execute arbitrary commands (CVE-2025-7850) and obtain root shell access (CVE-2025-7851) enables an attacker to perform silent, persistent malicious activities. This could include bypassing firewall rules, installing backdoors, stealing administrative credentials, redirecting traffic, or pivoting to other devices within the internal network, resulting in a full network and infrastructure compromise.

Successful exploitation of these vulnerabilities grants an attacker deep control of network infrastructure, which can be leveraged for a full system compromise. Potential malicious actions include installing persistent malware, redirecting network traffic, exfiltrating sensitive internal network data, or rendering the device completely inoperable, thus disrupting critical business functions. The security risk is significant and can lead to major data breaches and organizational downtime. The vulnerabilities impact a total of 13 Omada gateway product models. As such, all firmware versions prior to the latest fixed builds are considered vulnerable.

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- Cross-referencing your specific model and installed firmware version against the vendor's advisory to confirm vulnerability.
- Patching affected devices by installing the latest firmware.
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	omadanetworks, hhs, bleepingcomputer

Alert ID 10f196df

View Alert

Share Feedback

was this helpful?  | 

Tags CVE-2025-7851, CVE-2025-7850, Omada Gateways, TP-Link Devices

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

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**