VULNERABILITY BULLETINS

TP-Link Security Advisory Released (CVE-2025-6542 and CVE-2025-6541)

TLP:WHITE

Oct 22, 2025

On October 21, 2025, TP-Link issued a security advisory regarding multiple firmware versions of its Omada gateway devices to address two high-severity command injection flaws, CVE-2025-6542 and CVE-2025-6541.

The most critical vulnerability, CVE-2025-6542, has a CVSS score of 9.3 and can be exploited by a remote unauthenticated attacker to execute arbitrary OS commands on the underlying system. 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 affected products are TP-Link Omada gateways, which are full-stack networking solutions, serving as routers, firewalls, and VPN gateways, typically leveraged in small to medium businesses for centralized management. Given their role as network boundaries and

traffic controllers, these devices are high-value targets for threat actors. Exploiting a vulnerable gateway device allows attackers to compromise an organization’s network, leading to severe consequences such as data theft, lateral movement, and persistent access.

The two vulnerabilities are both arbitrary operating system (OS) command injection flaws. The first flaw, tracked as CVE-2025-6542, allows a remote unauthenticated attacker to exploit the vulnerability and execute commands on the gateway's operating system. The second flaw, CVE-2025-6541, is exploitable only by an attacker who has already managed to log in to the web management interface. These flaws represent a significant risk, as they both can allow threat actors to run unauthorized commands on the networking infrastructure.

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)	hhs, omadanetworks, bleepingcomputer

Alert ID 4f783191

View Alert

Share Feedback

was this helpful?  | 

Tags Omada Gateways, CVE-2025-6541, CVE-2025-6542, 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/**