مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in TP-Link Omada Gateways

Tracking #:432317837

Date:21-10-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that TP-Link Systems has released firmware updates addressing multiple critical and high-severity vulnerabilities in its Omada gateway series, including models ER605, ER7206, ER8411, and others used in enterprise and SMB networks.

TECHNICAL DETAILS:

Vulnerability Details

- CVE-2025-6542 (CVSS 9.3 – Critical)
  Remote unauthenticated command execution vulnerability allowing arbitrary OS commands.
- CVE-2025-6541 (CVSS 8.6 – High)
  Command execution vulnerability through the web management interface, requiring authentication.
- CVE-2025-7850 (CVSS 9.3 – Critical)
  Command injection flaw exploitable post-authentication via the web portal.
- CVE-2025-7851 (CVSS 8.7 – High)
  Vulnerability that could enable attackers with valid or compromised credentials to obtain root shell access under restricted conditions.

Successful exploitation of these vulnerabilities may result in full device compromise, configuration tampering, traffic interception, or deployment of persistent malware within enterprise and small business networks.

Affected Products and Fixed Versions

Model	Affected Versions	Fixed Version
ER8411	< 1.3.3 Build 20251013	≥ 1.3.3 Build 20251013 (Rel.44647)
ER7412-M2	< 1.1.0 Build 20251015	≥ 1.1.0 Build 20251015 (Rel.63594)
ER707-M2	< 1.3.1 Build 20251009	≥ 1.3.1 Build 20251009 (Rel.67687)
ER7206	< 2.2.2 Build 20250724	≥ 2.2.2 Build 20250724 (Rel.11109)
ER605	< 2.3.1 Build 20251015	≥ 2.3.1 Build 20251015 (Rel.78291)
ER706W / ER706W-4G	< 1.2.1 Build 20250821	≥ 1.2.1 Build 20250821 (Rel.80909 / Rel.82492)
ER7212PC	< 2.1.3 Build 20251016	≥ 2.1.3 Build 20251016 (Rel.82571)
G36	< 1.1.4 Build 20251015	≥ 1.1.4 Build 20251015 (Rel.84206)
G611	< 1.2.2 Build 20251017	≥ 1.2.2 Build 20251017 (Rel.45512)
FR365	< 1.1.10 Build 20250626	≥ 1.1.10 Build 20250626 (Rel.81746)
FR205	< 1.0.3 Build 20251016	≥ 1.0.3 Build 20251016 (Rel.61376)
FR307-M2	< 1.2.5 Build 20251015	≥ 1.2.5 Build 20251015 (Rel.76743)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by TP-Link.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://support.omadanetworks.com/en/document/108455/
- https://support.omadanetworks.com/en/document/108456/