مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Command Injection Vulnerabilities in TP-Link NVRs

Tracking #:432317518

Date:23-07-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed TP-Link has released security updates, addressing multiple high severity vulnerabilities in its Network Video Recorder models. The vulnerabilities may allow attackers to execute arbitrary operating system commands on the affected devices, potentially leading to full system compromise.

TECHNICAL DETAILS:

TP-Link has issued a security advisory addressing two high severity vulnerabilities, **CVE-2025-7723** and **CVE-2025-7724**, affecting its VIGI NVR1104H-4P V1 and VIGI NVR2016H-16MP V2 devices.

These vulnerabilities involve both authenticated and unauthenticated OS command injections, which may allow attackers to execute arbitrary commands on the device's operating system. This could lead to full system compromise, data breaches, or unauthorized control of the NVRs.

Vulnerability Details:

- **CVE-2025-7723:**
  - **CVSS v4.0 Score:** 8.5 / High

- **CVE-2025-7724:**
  - **CVSS v4.0 Score:** 8.7 / High

Affected Product Model	Related Vulnerabilities	Affected Version	Fixed Version
VIGI NVR1104H-4P V1	CVE-2025-7723 CVE-2025-7724	< 1.1.5 Build 250518	1.1.5 Build 250518
VIGI NVR2016H-16MP V2	CVE-2025-7723 CVE-2025-7724	< 1.3.1 Build 250407	1.3.1 Build 250407

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the latest updates 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://www.tp-link.com/us/support/faq/4547/