مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates- Zyxel Networking Devices

Tracking #:432318458

Date:25-02-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

ADVISORY

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Zyxel has released security patches addressing multiple vulnerabilities impacting its 4G LTE/5G NR CPE devices, DSL/Ethernet routers, Fiber ONTs, and Wireless Extenders.

TECHNICAL DETAILS:

Zyxel has released urgent security patches addressing multiple vulnerabilities impacting its 4G LTE/5G NR CPE devices, DSL/Ethernet routers, Fiber ONTs, and Wireless Extenders.

Vulnerability Details

1. **CVE-2025-13942 — Critical (CVSS 9.8)**
   - **Type:** Unauthenticated Command Injection
   - **Component:** UPnP (Universal Plug and Play) Function

2. **CVE-2025-13943 — High (CVSS 8.8)**
3. **CVE-2026-1459 — High (CVSS 7.2)**

4. **Denial-of-Service Vulnerabilities (Moderate – CVSS 4.9)**
   - CVE-2025-11845
   - CVE-2025-11846
   - CVE-2025-11847

RECOMMENDATIONS:

- Immediate Actions:
  - Apply the latest firmware updates from Zyxel.
  - Verify patch levels across all deployed models.

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.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-null-pointer-dereference-and-command-injection-vulnerabilities-in-certain-4g-lte-5g-nr-cpe-dsl-ethernet-cpe-fiber-onts-security-routers-and-wireless-extenders-02-24-2026