مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in NETGEAR Wi-Fi Routers and Access Points

Tracking #:432316838

Date:07-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in NETGEAR Wi-Fi routers and access points that could be exploited to gain complete control of the affected devices.

TECHNICAL DETAILS:

NETGEAR has recently issued security advisories addressing critical vulnerabilities in several of its Wi-Fi router and access point models.

Vulnerabilities Details:

- **CVE-2025-25246**
    - CVSS score 9.8 Critical
    - A critical unauthenticated remote code execution (RCE) vulnerability exists in NETGEAR Wi-Fi routers. This vulnerability could allow an attacker to take complete control of the affected device without requiring login credentials.
- **Impacted Router Models and Fixed Firmware Versions:**
    - **XR1000 –** Fixed in firmware **1.0.0.74**
    - **XR1000v2 –** Fixed in firmware **1.1.0.22**
    - **XR500 –** Fixed in firmware **2.3.2.134**

- **PSV-2024-0117**
    - CVSS score 9.6 Critical
    - A critical authentication bypass vulnerability exits in NETGEAR access points. This flaw could permit an unauthorized user to bypass authentication and gain access to the device's administrative interface.
- **Impacted Access Point Models and Fixed Firmware Versions:**
    - **WAX206 –** Fixed in firmware **1.0.5.3**
    - **WAX220 –** Fixed in firmware **1.0.3.5**
    - **WAX214v2 –** Fixed in firmware **1.0.2.5**

RECOMMENDATIONS:

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

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://kb.netgear.com/000066558/Security-Advisory-for-Unauthenticated-RCE-on-Some-WiFi-Routers-PSV-2023-0039
- https://kb.netgear.com/000066557/Security-Advisory-for-Authentication-Bypass-on-Some-Wireless-Access-Points-PSV-2024-0117