مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Netgear Wi-Fi Range Extender

Tracking #:432317214

Date:05-05-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in Netgear Wi-Fi range extender that could allow remote attackers to gain unauthorized access to the device and potentially steal sensitive data or execute arbitrary code.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-4148**
  - **Severity:** High (CVSS v3.1 score: 8.8)
  - A buffer overflow vulnerability exists in the sub_503FC function due to improper validation of the host argument. Remote attackers can exploit this flaw to overwrite memory, leading to arbitrary code execution, full device compromise, and data theft. The vulnerability is remotely exploitable and does not require user interaction.
- **CVE-2025-4149**
  - **Severity:** High (CVSS v3.1 score: 8.8)
  - This vulnerability affects the sub_54014 function, which mishandles the host parameter. Exploitation allows attackers to bypass security controls, gain remote access, and potentially install malware or steal data. The attack can be launched remotely without authentication.
- **CVE-2025-4150**
  - **Severity:** High (CVSS v3.1 score: 8.8)
  - A similar buffer overflow flaw is present in the sub_54340 function. Successful exploitation grants attackers unauthorized access to network traffic and stored credentials, with the potential for full device compromise. The vulnerability is remotely exploitable and does not require user interaction.

- **Affected Product:** Netgear EX6200 Wi-Fi Range Extender
- **Affected Firmware Version:** 1.0.3.94

RECOMMENDATIONS:

- **Disable remote management** features to reduce the attack surface.
- **Restrict network access** to the device and segment critical systems from the vulnerable extender.
- **Monitor device logs** for unusual or unauthorized activity.
- **Regularly check for firmware updates** and apply patches as soon as they become available.
- **Consider replacing or isolating** affected devices, especially in high-risk or sensitive environments.

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.cve.org/CVERecord?id=CVE-2025-4148
- https://www.cve.org/CVERecord?id=CVE-2025-4149
- https://www.cve.org/CVERecord?id=CVE-2025-4150