مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in NETGEAR Routers

Tracking #:432316732

Date:13-01-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in NETGEAR routers that is being actively exploited in the wild. This vulnerability allows attackers to gain unauthorized access and execute malicious code on affected devices.

TECHNICAL DETAILS:

Vulnerability Details

- CVE-2024-12847
- CVSS score 9.8 Critical
- A critical security vulnerability exists in several NETGEAR router models, allowing remote attackers to gain unauthorized access and execute arbitrary commands with root privileges. This vulnerability has been actively exploited in the wild.
- The vulnerability stems from improper authentication checks in the router's embedded web server. Attackers can bypass authentication by using URLs containing the substring "currentsetting.htm", allowing them to interact with the router's backend services without credentials
- Successful exploitation allows attackers to:
    - Gain unauthorized root-level access to affected routers
    - Execute arbitrary operating system commands
    - Intercept or modify network traffic
    - Use compromised routers as pivot points for further attacks

Affected Devices:

- NETGEAR DGN1000: Firmware versions below 1.1.00.48
- NETGEAR DGN2200 v1: All firmware versions
- Other NETGEAR devices may also be vulnerable

Mitigations:

- For NETGEAR DGN1000: Update firmware to version 1.1.00.48 or later
- For NETGEAR DGN2200 v1: Replace with newer, supported models as no security updates are available

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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://nvd.nist.gov/vuln/detail/CVE-2024-12847