مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in NETGEAR Routers

Tracking #:432317307

Date:26-05-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in NETGEAR wireless routers that could be exploited to gain unauthorized access to affected devices.

TECHNICAL DETAILS:

Vulnerabilities Details:

- CVE-2025-4978
- Severity: Critical (CVSSv4: 9.3)
- A critical authentication bypass vulnerability exists in the NETGEAR DGND3700v2 router. The flaw allows unauthenticated remote attackers to gain full administrative access through a hidden backdoor in the embedded HTTP server.
- Successful exploitation can lead to total network compromise, including credential theft, DNS hijacking, and persistent malware installation.

Affected Product:

- NETGEAR DGND3700v2 Wireless Router

Affected Version:

- Firmware V1.1.00.15_1.00.15NA

Fixed Versions:

- Firmware V1.1.00.26 or Later

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://nvd.nist.gov/vuln/detail/CVE-2025-4978