مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in NETGEAR Product

Tracking #:432315918

Date:03-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a High- Severity Vulnerability in Netgear product that could be exploited to gain unauthorized access to affected devices.

TECHNICAL DETAILS:

Vulnerability Details:

- **PSV-2024-0008**
- CVSS Score 8.8 High
- The vulnerability is due to missing function-level access control, which could allow unauthorized users to access and potentially exploit functionalities they shouldn't have access to.
- The Netgear NMS300 devices lack proper access control mechanisms for specific functions. This vulnerability could be exploited by an attacker to gain unauthorized access to functionalities within the device, potentially allowing them to:
  - Modify configurations
  - Disrupt device operations
  - Gain unauthorized access to sensitive data

Affected Products:

- Netgear NMS300 devices

Fixed Version:

- NMS300 version 1.7.0.37

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/000066192/Security-Advisory-for-Missing-Function-Level-Access-Control-on-the-NMS300-PSV-2024-0008