مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Multiple Vulnerabilities in NETGEAR XR1000 Series Routers

Tracking #:432316488

Date:08-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed NETGEAR has issued security advisories addressing two high-severity vulnerabilities in the XR1000 and XR1000v2 router models.

TECHNICAL DETAILS:

NETGEAR has issued security advisories addressing two high-severity vulnerabilities in the XR1000 and XR1000v2 router models.

1. Sensitive Information Disclosure Vulnerability, CVSS: 7.8 (High)
   - Affected Models: NETGEAR XR1000
   - Firmware Fixed: Version 1.0.0.74

2. Post-Authentication Command Injection ,CVSS: 8.2 (High)
   - Affected Models:
     - NETGEAR XR1000
     - NETGEAR XR1000v2

   Firmware Fixed:
     - XR1000: Version 1.0.0.74
     - XR1000v2: Version 1.1.1.22

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update to latest Firmware Versions for affected routers.

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/000066408/Security-Advisory-for-Sensitive-Information-Disclosure-on-Some-Routers-PSV-2023-0117
- https://kb.netgear.com/000066409/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-Routers-PSV-2023-0109