مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerabilities in NETGEAR Products

Tracking #:432316818

Date:03-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed NETGEAR has addressed two critical security vulnerabilities in its products, which could allow unauthenticated attackers to execute arbitrary code or remotely exploit devices.

TECHNICAL DETAILS:

NETGEAR has addressed two critical security vulnerabilities in its products, which could allow unauthenticated attackers to execute arbitrary code or remotely exploit devices.
These vulnerabilities affect multiple models, including the XR series routers and WAX series access points. Both vulnerabilities have been rated as critical, with CVSS scores of 9.8 and 9.6 respectively. NETGEAR has released firmware updates to mitigate these risks, and it is strongly recommended that affected users update their devices to the latest firmware versions immediately to prevent potential exploitation.

1. Unauthenticated Remote Code Execution Vulnerability (RCE) in NETGEAR XR Series Routers

- **Affected Models:**
  - XR1000 (fixed in firmware version 1.0.0.74)
  - XR1000v2 (fixed in firmware version 1.1.0.22)
  - XR500 (fixed in firmware version 2.3.2.134)
- **Vulnerability Overview:** This critical vulnerability allows unauthenticated remote attackers to execute arbitrary code on the affected NETGEAR XR series routers. The issue arises from insufficient validation in the device's remote management functionality, which can be exploited without authentication. If successfully exploited, attackers could gain remote access to the affected devices and potentially take control of the system, executing arbitrary commands or code with high privileges.
- **CVSS Score:** Critical: CVSS 3.0 Score: 9.8

2. Remote Exploitation Vulnerability in NETGEAR WAX Series Access Points

- **Affected Models:**
  - WAX206 (fixed in firmware version 1.0.5.3)
  - WAX220 (fixed in firmware version 1.0.3.5)
  - WAX214v2 (fixed in firmware version 1.0.2.5)
- **Vulnerability Overview:** This critical remote exploitation vulnerability allows attackers to remotely execute commands on the affected NETGEAR WAX series access points. The flaw in the remote management functionality exposes the devices to remote attackers, allowing them to exploit the vulnerability without requiring user interaction or authentication. Successful exploitation could lead to a complete compromise of the access points, affecting network infrastructure and performance.
- **CVSS Score:** Critical: CVSS 3.1 Score: 9.6

RECOMMENDATIONS:

- All users of the affected NETGEAR models (XR series routers and WAX series access points) should update their devices to the latest firmware versions to mitigate the risks posed by these vulnerabilities.

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/000066558/Security-Advisory-for-Unauthenticated-RCE-on-Some-WiFi-Routers-PSV-2023-0039
- https://kb.netgear.com/000066557/Security-Advisory-for-Remote-Exploitation-on-Some-Wireless-Access-Points-PSV-2021-0117