# AL2025_08 Netgear warns users to patch critical WiFi router vulnerabilities (11th February 2025)

### Description

Netgear has identified and patched two critical vulnerabilities affecting multiple WiFi router models, including WiFi 6 access points (WAX206, WAX214v2, and WAX220) and Nighthawk Pro Gaming routers (XR1000, XR1000v2, XR500). These vulnerabilities allow unauthenticated threat actors to exploit remote code execution (RCE) and authentication bypass issues. Netgear strongly recommends users update their devices to the latest firmware to mitigate potential risks.

### Attack Details

The security flaws, tracked internally as PSV-2023-0039 (Remote Code Execution) and PSV-2021-0117 (Authentication Bypass), enable attackers to take control of vulnerable routers without user interaction. These low-complexity exploits pose a severe risk as they allow cybercriminals to execute arbitrary code remotely or gain unauthorized access to the device. While Netgear has not disclosed the precise technical details of the vulnerabilities, similar past exploits have been leveraged to install malware, exfiltrate data, or launch further network attacks.

### Remediation

To protect against potential exploitation, users must promptly update their Netgear routers to the latest firmware versions. The following steps should be taken:

1. **Check Router Model & Firmware Version:**
   - XR1000: Firmware version 1.0.0.74
   - XR1000v2: Firmware version 1.1.0.22
   - XR500: Firmware version 2.3.2.134
   - WAX206: Firmware version 1.0.5.3
   - WAX220: Firmware version 1.0.5.3
   - WAX214v2: Firmware version 1.0.2.5
2. **Update Firmware:**
   - Visit Netgear Support
   - Enter the router model number in the search box
   - Select the corresponding model and navigate to the Downloads section
   - Choose the latest firmware version under Current Versions
   - Follow the release notes for installation instructions
3. **Additional Security Measures:**
   - Disable remote management unless necessary
   - Change default login credentials to strong, unique passwords
   - Regularly monitor router logs for suspicious activity
   - Implement a firewall and enable network encryption

Netgear has emphasized that failing to apply the necessary patches could leave users vulnerable to attacks. Users must follow the remediation steps immediately to secure their devices against potential exploits. The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

**References**

- Gatlan, S. (2025, February 4). Netgear warns users to patch critical WiFi router vulnerabilities. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/netgear-warns-users-to-patch-critical-wifi-router-vulnerabilities/
- Paganini, P. (2025, February 4). Netgear urges users to upgrade two flaws impacting WiFi router models. Retrieved from Security Affairs. https://securityaffairs.com/173839/security/netgear-wifi-routers-flaws.html