## Pakistan Telecom Authority Headquarters, Islamabad

**PTA Cyber Security Advisory No: 143** **22-09-2021**

**Name:** Vulnerability in Several Netgear Router Models

**Threat Classification:** Remote code execution

**Affected Products/ Models:**

- **R6400v2**
- **R6700**
- **R6700v3**
- **R6900**
- **R6900P**
- **R7000**
- **R7000P**
- **R7850**
- **R7900**
- **R8000**
- **RS400**

**Summary:**

Vulnerability is found which exists in **Circle**, a third-party component included in the firmware that offers **parental control features**. With the Circle update daemon enabled to run by default even if the router hasn't been configured to limit daily internet time for websites and applications. This results in a scenario that can permit bad actors with network access to gain remote code execution (RCE) as root via a **Man in the Middle attack (MitM**) which gives the attacker the ability to overwrite executable binaries with malicious code.

| Severity | High |
|---|---|
| **Attack Vector** | Network |
| **Privileges required** | None |

For further details, please visit following link:
https://kb.netgear.com/000064039/Security-Advisory-for-Remote-Code-Execution-on-Some-Routers-PSV-2021-0204

**Recommendations:**

- Please visit the website link for remediation for the aforementioned vulnerabilities: https://kb.netgear.com/000064039/Security-Advisory-for-Remote-Code-Execution-on-Some-Routers-PSV-2021-0204

- **NETGEAR** strongly recommends that you download the latest firmware as soon as possible.
- If your product is supported by one of our apps, using the app is the easiest way to update your firmware:
  - Orbi products: NETGEAR Orbi app.
  - NETGEAR WiFi routers: NETGEAR Nighthawk app.
  - Some NETGEAR Business products: NETGEAR Insight app (firmware updates through the app are available only for Insight subscribers).
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- Designate a PoC from your security / Network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.