VULNERABILITY BULLETINS

Netgear Vulnerability Impacts Thousands of Routers; Possible Medical Equipment Impact

TLP:WHITE

Sep 23, 2021

Security researchers have discovered a vulnerability in a pre-installed component of several Netgear routers. The vulnerability, designated CVE-2021-40847, is related to third-party parental control software Circle, which is designed and developed by the Disney Corporation. The optional software, even if it was not utilized, came pre-installed on several types of Netgear routers.

Medical devices that might be affected by this vulnerability include:

- Portable X-ray equipment using wireless digital X-ray imaging detectors that rely on the affected routers.
- Fixed X-ray equipment using wireless digital X-ray imaging detectors that rely on the affected routers.
- Medical equipment that might contain an embedded affected wireless router or rely on the affected routers.

Users are encouraged to update their affected Netgear products, which are listed further into the alert, to their most current firmware version. Additional details and recommendations are also included within this alert.

According to security firm GRIMM, the update process of the Circle Parental Control Service on routers allows remote attackers with direct network access to gain remote code execution (RCE) as root via a Man-in-the-Middle (MitM) attack, by uploading a specifically crafted database file. This corrupted database file can give the attacker the ability to overwrite legitimate executable files with attacker-controlled code.

While the Circle parental controls themselves are not enabled by default on the routers, the Circle update daemon, designated circled, is enabled by default, thereby allowing actors to execute CVE-2021-40847 on routers that do not have Circle parental controls enabled.

The list of affected Netgear routers is listed below:

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

Reference(s)	Tom's Guide, Grimm-co, Netgear, PC Mag

CVE(s)

CVE-2021-40847

Recommendations

Healthcare administrators and individuals affected by the vulnerability are heavily encouraged to contact and consult with the appropriate medical device manufacturer before attempting to install the firmware updates. In regards to imaging devices affected by the vulnerability, failure to consult with the device manufacturer may result in defective images and unnecessary repeated patient exposure to ionizing (x-ray) radiation.

NETGEAR strongly recommends that you download the latest firmware as soon as possible. Firmware fixes are currently available for all affected products:

- R6400v2 fixed in firmware version 1.0.4.120
- R6700 fixed in firmware version 1.0.2.26
- R6700v3 fixed in firmware version 1.0.4.120
- R6900 fixed in firmware version 1.0.2.26
- R6900P fixed in firmware version 3.3.142_HOTFIX
- R7000 fixed in firmware version 1.0.11.128
- R7000P fixed in firmware version 1.3.3.142_HOTFIX
- R7850 fixed in firmware version 1.0.5.76
- R7900 fixed in firmware version 1.0.4.46
- R8000 fixed in firmware version 1.0.4.76
- RS400 fixed in firmware version 1.5.1.80

To download the latest firmware for the affected NETGEAR product:

1. Visit NETGEAR Support.
2. Start typing your model number in the search box, then select your model from the drop-down menu as soon as it appears.
3. Click Downloads.
4. Under Current Versions, select the first download whose title begins with Firmware Version.
5. Click Release Notes.
6. Follow the instructions in the firmware release notes to download and install the new firmware.

Other Recommendations:

Confirm with affected manufactures that all functions not required to directly support the medical device operation are disabled, such as:

- Plug and Play
- DMZs
- Wi-Fi Protected Setup (WPS)

Additional recommendations, provided by the Cybersecurity and Infrastructure Security Agency (CISA) Industrial Control Systems Computer Emergency Response Team (ICS-CERT) can be accessed here.

Sources

NETGEAR Support: Security Advisory for Remote Code Execution on Some Routers, PSV-2021-0204

PCMag: Thanks to Disney, 11 Netgear Routers Need to Be Patched Immediately

Tom’s Guide: Thousands of Netgear Routers Can Be Hacked — Here's What to Do

GRIMM: Mama Always Told Me Not to Trust Strangers without Certificates

Alert ID 1112b037

View Alert

Tags Netgear vulnerabilities, NETGEAR Nighthawk, Netgear Routers, Netgear Products

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC’s Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**