View on GitHub

# Netgear Nighthawk Firmware Update Vulnerability

The router Netgear Nighthawk R7000 does not validate Netgear's TLS server certificate when performing a firmware update. This allows an attacker with access to the upstream network to assume a TLS man-in-the-middle position and thereby deliver compromised firmware updates to the router. Furthermore, if the update server can not be reached via HTTPS, the router will automatically fall back to an unencrypted FTP connection. This vulnerability affects both manual updates via the web interface and automatic firmware updates.

| | |
|---|---|
| **Title** | **Netgear Nighthawk Firmware Update Vulnerability** |
| Product | Netgear Nighthawk R7000 WLAN-Router AC1900 |
| Vulnerable firmware versions | *V1.0.9.6_1.2.19 - V1.0.11.100_10.2.100* |
| CVE number | CVE-2020-13245, CVE-2020-35800 |
| Vendor advisory | PSV-2020-0112 |
| Vendor website | https://www.netgear.com |
| Identified in | December 2019 |
| Identified by | IoT Lab, University of Applied Sciences Upper Austria, Campus Hagenberg |
| Website | https://www.fh-ooe.at/si/ |
| Team | Simon Birngruber BSc (FH OÖ Campus Hagenberg) |
| | Ing. Florian Hehenberger BSc (FH OÖ Campus Hagenberg) |
| | Paul Gründlinger (FH OÖ Campus Hagenberg) |
| | DI Markus Zeilinger (FH OÖ Campus Hagenberg) |
| | Dieter Vymazal BSc MSc (FH OÖ Campus Hagenberg) |
| | Florian Hehenberger |
| Contact Information | florian.hehenberger@students.fh-hagenberg.at<br>PGP Fingerprint: F48B DFAD 1B38 442A 1686 920C BF29 14FA 4A71 ECE7 |

## Vendor description

*„At NETGEAR, we turn ideas into innovative networking products that connect people, power businesses, and advance the way we live. Easy to use. Powerful. Smart. And designed just for you."*

Source: https://www.netgear.com/about

## Vulnerability overview

The Netgear R7000 router firmware retrieves new firmware updates from the update server *https://http.fw.updates1.netgear.com*. First, the currently installed firmware version is compared with the version number in the file */r7000/ww/fileinfo.txt* on the update server. If the installed version number is lower, the router assumes that a new firmware version is available and the firmware update is downloaded from the update server and installed on the router. The firmware is not signed cryptographically. A firmware update includes release notes (*/r7000/ww/stringtable.dat*), language files (*/r7000/ww/R7000-*-Language-table*) and the firmware image itself (*/r7000/ww/R7000-V1.0.XXX.*.chk*). The HTTP connection used is protected by TLS, but the certificate of the update server is not checked by the router. An analysis of the firmware showed that the router uses the widely used program *wget* with the parameter *–no-check-certificate* when downloading the firmware image from the update server. This behavior allows an attacker to perform a man-in-the-middle attack and to mimic the position of the update server. Furthermore, the lack of an authenticity and integrity check of the firmware image itself on the router enables an attacker to provide manipulated firmware updates that are installed by the router after the download.

If individual files or the update server itself are not available, the router tries to download the update via FTP from *updates1.netgear.com*. This connection is unencrypted and offers an attacker additional attack vectors.

An automatic update function for firmware updates is available since firmware version *V1.0.9.6_1.2.19*. If a user connects to the router's web interface for the first time after an update to firmware version *V1.0.9.6_1.2.19* or later, she/he is asked to choose whether firmware updates should be downloaded and installed automatically in the future. When the user decides to activate the automatic update function, an attacker is able to install manipulated firmware updates without any need for further user interaction which increases the criticality of the vulnerability.

## Proof of Concept

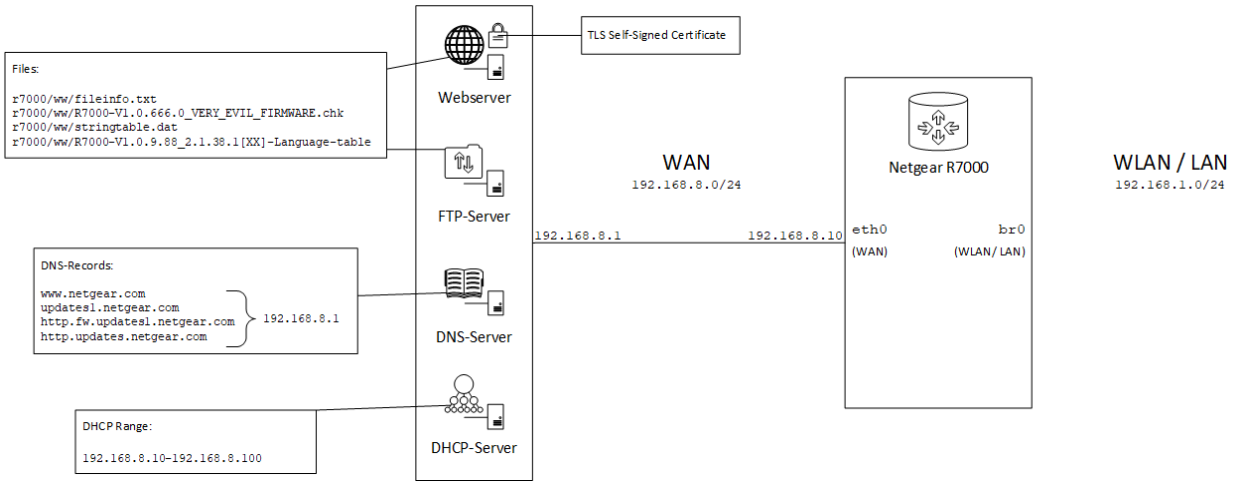


*Figure 1: PoC setup for the TLS MitM attack, the attacker is controlling the WAN services like DHCP, DNS and the (fake) update server*

In our proof of concept, the router R7000 is first updated to firmware version *V1.0.11.100_10.2.100* and then reset to factory settings. During the initial setup via the web interface, the option "Automatically update to future firmware" is selected. As shown in Figure 1, the attacker operates a DHCP, DNS, FTP and web server with the IP address *192.168.8.1* directly connected to the WAN port of the router. The DHCP server provides an IP address for the router's WAN interface (the router is configured as a DHCP client on the WAN port by default) and distributes the attacker's DNS server (*192.168.8.1*) as primary DNS server. The DNS server resolves the hostnames *www.netgear.com*, *updates1.netgear.com*, *http.fw.updates1.netgear.com* and *http.updates.netgear.com* to the IP address (*192.168.8.1*) of the attacker's server. The files required for the firmware update are stored both on the web server and on the FTP server in the same directory as on the original Netgear update server (*/r7000/ww/*). The file *R7000-V1.0.666.0_VERY_EVIL_FIRMWARE.chk* is shown as the latest firmware version in the file *fileinfo.txt* and is made available on the attacker's server. When the router checks for an available update, it is referenced to the attacker's server by spoofing the DNS records. Then the router checks if the firmware version number offered on the attacker's server is higher than the version number of the installed firmware. This check causes the router to download and install the manipulated firmware. If the web server is not available, the manipulated firmware update takes place via the attacker's FTP server.

The "malicious" demo firmware used in our proof of concept is a manipulated original firmware image (version *V1.0.9.88_10.2.88*), whereby the company logo of Netgear has been replaced for illustration purposes, as shown in Figure 2.

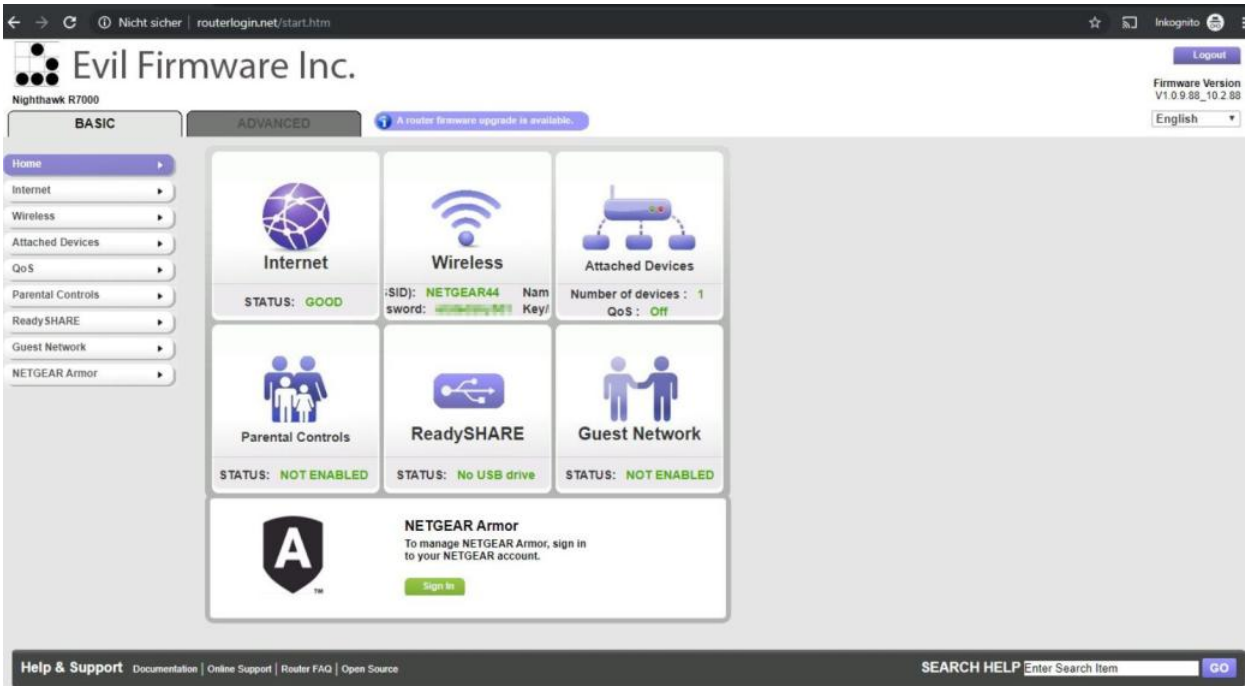

*Figure 2: The router web interface after a successful automatic firmware update to a manipulated firmware version*

## Vulnerable devices and firmware versions

The auto update function for the Netgear R7000 router is available since firmware version *V1.0.9.6_1.2.19*. With our proof of concept we were able to verify the vulnerability in all versions from *V1.0.9.6_1.2.19* up to version *V1.0.11.100_10.2.100*.

After a string analysis of the firmware of some other Netgear models, we suspect the following models to be vulnerable too:

- Netgear R6120
- Netgear R6220
- Netgear R6350
- Netgear R6400, Netgear R6400v2
- Netgear R6800
- Netgear R6850
- Netgear R7000P
- Netgear R7800
- Netgear R8000
- Netgear R9000
- Netgear RAX120
- Netgear RBR20
- Netgear XR300
- Netgear XR500

## Workaround

Owners of affected devices can take the following steps to mitigate the vulnerability:

- Disable automatic firmware updates
- Do not update the router via the firmware update assistant in the web interface

Owners of affected devices can take the following steps to update the firmware on their device:

- Manually download new firmware images from the official Netgear support website at *https://www.netgear.com/support/product/R7000#download*
- Manually upload and install the firmware image on the router via the web interface.

## Solution

The vulnerability can only be remedied by a firmware update from Netgear.

## Communication timeline

| ***Date*** | ***Action*** |
|---|---|
| 08.01.2020 | Tried to contact Netgear with support of the german *Cert-Bund*. |
| 28.01.2020 | Contacted @Netgear and @Bugcrowd via Twitter. |
| 29.01.2020 | Received replies from @Netgear and @Bugcrowd on Twitter. |
| 29.01.2020 | Received an email from the Netgear Product Security Incident Response Team (Netgear PSIRT). |
| 29.01.2020 | Sent the advisory to Netgear PSIRT. |
| 29.01.2020 | Received an email from Netgear PSIRT confirming the receipt of the advisory and asking for our disclosure timeline. Also Netgear PSIRT agreed to keep us up to date on the mitigation process. |
| 30.01.2020 | Submission of our 90 day public disclosure policy (starting with 29.01.2020) to Netgear PSIRT. |
| 09.04.2020 | Sent an email to Netgear PSIRT asking about the current mitigation status, no reply. |
| 26.05.2020 | Public disclosure on github |

## Version history

| ***Date*** | ***Version*** | ***Changes*** |
|---|---|---|
| 20.12.2019 | V 1.0 | Initial Commit. |
| 22.04.2020 | V 1.1 | Confirmed the vulnerability in the latest firmware version *V1.0.11.100_10.2.100*, Added communication timeline. |
| 11.04.2021 | V 1.2 | Added vendor advisory and vendor CVE. |

Netgear Nighthawk Firmware Update Vulnerability maintained by IoT-Lab-FH-OOE

Published with GitHub Pages