Two vulnerabilities regarding firmware updates in Netgear WPN824EXT WiFi Range Extender.

Affected products

We have tested on WPN824EXT WiFi Range Extender (firmware version: 1.1.1_1.1.9 and earlier). Also, we suspect it may also work on other models with similar firmware versions.

Vulnerability #1 - Firmware downgrade attack

Overview:

An exploitable firmware downgrade vulnerability was discovered on the WPN824EXT WiFi Range Extender. An attacker can conduct a MITM attack to replace the user-uploaded firmware image with an original old firmware image.

Details:

When performing a firmware update, users can download a new firmware image from the vendor server and upload it via the web interface of the device. It is worth noting that, when a new firmware image is uploaded, the device checks the version of the uploaded firmware by reading the file name and extracting the firmware version from the file name. However, if an old firmware is uploaded with a file name from a new firmware image, the firmware verification can be passed.

Note that the communication uses the plain HTTP protocol, which does not provide any cryptographic protection of the uploaded contents. An attacker with a privileged network position (which could be obtained via ARP spoofing, DNS spoofing, or other approaches) can exploit this issue in order to provide firmware update images with lower versions. Specifically, the attacker can change uploaded contents to the contents of an old firmware image without changing the file name field in the network package after a user uploads a new firmware image. In this case, the user will think that they are installing a newer version of firmware when in reality the old firmware is installed on the device. This could allow more vulnerabilities in old versions of firmware to be introduced.

The backend logs after launching the attack are listed below. From the logs, we can see that after the firmware image is replaced, the firmware verification can be passed and the firmware update process proceeds as if a new firmware image is uploaded.

```
/tmp/netgear-wpn824ext-image crc_check ok ...
begin to write kernel and rootfs, offset: 325
Unlocking /dev/mtd/3 ...
Writing from /tmp/netgear-wpn824ext-image to /dev/mtd/3 ...  [ ]w: 16384
[w]w: 32768
[w]w: 49152
[w]w: 65536
[w]w: 81920
[w]w: 98304
[w]w: 114688
[w]w: 131072
[w]w: 147456
[w]w: 163840
[w]w: 180224
[w]w: 196608
[w]w: 212992
[w]w: 229376
[w]w: 245760
[w]w: 262144
[w]w: 278528
[w]w: 294912
...
sys_reboot[PID: 813 (reboot)]: magic1:fee1dead, magic2:28121969, cmd:89abcdef
```

Vulnerability #2 - Firmware modification attack

Overview:

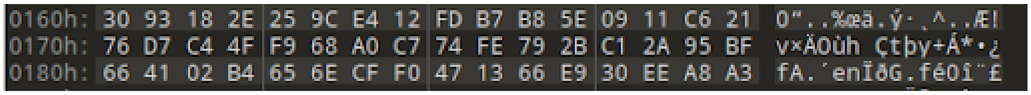
An exploitable firmware modification vulnerability was discovered on the WPN824EXT WiFi Range Extender. An attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the CRC check. A successful attack can either introduce a backdoor to the device or make the device DoS.

Details:

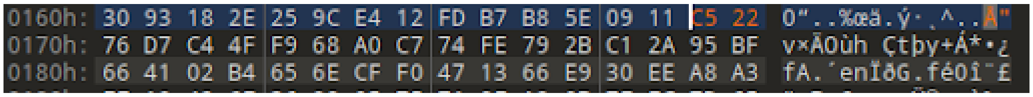
The data integrity check mechanism of the firmware update function is based on the CRC check. However, such a check is easy to be bypassed. Specifically, An attacker could customize a malicious firmware image with the CRC checksum equal to 0. Thus the data integrity check can be passed.

Also, the communication uses the plain HTTP protocol, which does not provide any cryptographic protection of the uploaded contents. An attacker with a privileged network position (which could be obtained via ARP spoofing, DNS spoofing, or other approaches) can exploit this issue in order to provide malicious firmware update images. Specifically, the attacker can change uploaded contents to the contents of a customized malicious firmware image after a user uploads a new firmware image. In this case, the user will think that they are installing a normal firmware image when in reality the malicious firmware is installed on the device. This could result in either DoS or backdoor attacks.

A simple example is given as figures below where the original firmware image and the modified firmware image are shown. The modified firmware image can be uploaded and flashed into the device successfully.



```
0160h: 30 93 18 2E 25 9C E4 12 FD B7 B8 5E 09 11 C6 21  0“..%œä.ý·¸^..Æ!
0170h: 76 D7 C4 4F F9 68 A0 C7 74 FE 79 2B C1 2A 95 BF  v×ÄOùh Çtþy+Á*•¿
0180h: 66 41 02 B4 65 6E CF F0 47 13 66 E9 30 EE A8 A3  fA.´enÏðG.fé0î¨£
```



```
0160h: 30 93 18 2E 25 9C E4 12 FD B7 B8 5E 09 11 C5 22  0“..%œä.ý·¸^..Å"
0170h: 76 D7 C4 4F F9 68 A0 C7 74 FE 79 2B C1 2A 95 BF  v×ÄOùh Çtþy+Á*•¿
0180h: 66 41 02 B4 65 6E CF F0 47 13 66 E9 30 EE A8 A3  fA.´enÏðG.fé0î¨£
```

The backend logs after launching the attack are listed below. From the logs, we can see that after the firmware image is replaced, the firmware verification can be bypassed and the firmware update process proceeds as if a normal firmware image is uploaded.

```
/tmp/netgear-wpn824ext-image crc_check ok ...
begin to write kernel and rootfs, offset: 324
Unlocking /dev/mtd/3 ...
Writing from /tmp/netgear-wpn824ext-image to /dev/mtd/3 ...  [ ]w: 16384
[w]w: 32768
[w]w: 49152
[w]w: 65536
[w]w: 81920
[w]w: 98304
[w]w: 114688
[w]w: 131072
[w]w: 147456
[w]w: 163840
[w]w: 180224
[w]w: 196608
[w]w: 212992
[w]w: 229376
[w]w: 245760
[w]w: 262144
[w]w: 278528
[w]w: 294912
[w]w: 311296
[w]w: 327680
[w]w: 344064
[w]w: 360448
[w]w: 376832
[w]w: 393216
[w]w: 409600
[w]w: 425984
[w]w: 442368
[w]w: 458752
[w]w: 475136

...
sys_reboot[PID: 880 (reboot)]: magic1:fee1dead, magic2:28121969, cmd:89abcdef
```