https://doi.org/10.2352/ISSN.2470-1173.2021.3.MOBMU-135

Firmware Vulnerability Analysis of Widely Used Low-Budget TP-Link Routers

***Franziska Schwarz*[1] *, Klaus Schwarz*[2,3] *, Daniel Fuchs*[1] *, Reiner Creutzburg*[1,2] *, David Akopian*[3]

[1] ***Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, Magdeburger Str. 50, D-14770 Brandenburg, Germany***

[2] ***SRH Berlin University of Applied Sciences, Berlin School of Technology, Ernst-Reuter-Platz 10, D-10587 Berlin, Germany***

[3] ***The University of Texas at San Antonio, College of Engineering, 1 UTSA Circle, San Antonio, TX 78249-0669, USA***

{***franziska.schwarz|daniel.fuchs|creutzburg***}***@th-brandenburg.de,*** {***klaus.schwarz|reiner.creutzburg***}***@srh.de, akopian@utsa.edu***

Abstract

TP-Link Technologies Co, Ltd. is a Chinese manufacturer of networking products and has a 42% share of the consumer WLAN market, making it the market leader. The company sells about 150 million devices per year. Many people worldwide use the Internet every day and are connected to the Internet with their computers. In the world of smart homes, even coffee machines, refrigerators, smart sockets, and light bulbs have found their way to the Internet, not to mention the many smartphones, which are, of course, also connected to the Internet. Since many different dangers come from a heater or printer and the many other smart devices directly connected to the Internet, there is a safe haven: the local area network. To connect to the Internet, one needs a modem, which is built into a router in many cases. Routers route network packets back and forth between several computer networks. They are used to connect to the Internet, and they are the bridge between the home network and the Internet in almost every household connected to the Internet. Because of their nature as a bridge between local and global networks, they are also the largest attack vector. [19] This paper examines how up-to-date the firmware of standard home network routers is and how secure the firmware is. In order to obtain a representative result, the examined routers were selected according to fixed rules. Each router had to be a product of the manufacturer TP-Link, the routers had to be in the low-budged range (less than 20 Euro) and be available from Amazon. Also, two different types of investigations were identified for the selected devices. Firstly, the devices were examined in the form of physically existing hardware, and secondly, an attempt was made to access the firmware via the manufacturer's website. It was found that even the fixing of current vulnerabilities and recently released update files are no guarantee that older vulnerabilities have been fixed. Secrets such as private keys and certificates are hard-coded in the firmware and can be extracted from update files. Moreover, devices are deliberately built to make it impossible to install the latest alternative firmware.

Introduction

Billions of households around the world are connected to the Internet. Many people all over the world use the Internet every day and are not only connected to the Internet with their computers. In the world of smart homes, even coffee machines, refrigerators, smart sockets, and light bulbs have made it to the Internet. Not to mention the many smartphones that are, of course, also connected to the Internet. As there are many different dangers to putting a heater or printer and the many other smart devices directly into the Internet, there is a safe haven: the local area network. To connect to the Internet, one needs a modem, which is built into a router in many cases. Routers route network packets back and forth between several computer networks. They are used to connect to the Internet and form the bridge between the home network and the Internet in virtually every home connected to the Internet. By nature, as a bridge between local and global networks, they also form the largest attack vector. Since June 2017, the Funkanlagengesetz (FuAG), adopted Europe-wide in Directive (2014/35/EU), has been in force in Germany. With this new law, stricter product-legal safety requirements apply to all electrical and electronic devices that emit or receive radio waves for radio communication or location, particularly mobile phones, Bluetooth devices, and WLAN routers. It states that no firmware from other manufacturers may be transferred by radio to a device affected by the Radio Equipment Act. Since many manufacturers are afraid of securing their devices accordingly, the entire update functionality for third-party firmware is suspended. In the past, this has led to orphaned routers and serious security vulnerabilities, and the takeover and aggregation of millions of routers in so-called botnets. This paper will investigate how up-to-date the firmware is on standard home network routers and how secure the firmware is.

Basics

To sufficiently examine a router for its security, many basics are necessary, which will be clarified in the following section.

Router

Routers are network devices that can forward network packets between several computer networks. They are most often used for Internet connection, the secure coupling of several locations (Virtual Private Network), or direct coupling of several local network segments. Many routers also translate between private and public IP addresses or map firewall functions using a set of rules.

TP-Link

As a manufacturer of network products, smart home devices, and telephones for home, small and medium businesses, TP-Link was established in 1996 in Shenzhen, China. To this day, the company's headquarters is also located there. The company claims to have sold over 150 million devices worldwide in 2017 alone. Besides, TP-Link has a 42% share of the consumer WLAN market and is the market leader [15].

Botnet

A botnet consists of several devices connected to the Internet, each of which operates a bot. A bot is a software application that automates tasks. Botnets are usually used to perform attacks such as the Distributed Denial of Service attack [12]. The operator of a botnet usually controls it from a command and control server. Zombies are devices connected to the Internet and are illegally taken over by vulnerabilities and without the owner's knowledge. In this thesis, a negative interpretation of the term "botnet" is assumed. In the sense of the thesis, a botnet is; therefore, a device connected to a network such as the Internet, which has been taken over by unlawfully exploiting vulnerabilities to use its computing power for malicious purposes [12].

Binwalk

Binwalk is a tool for exploring a given binary image for embedded files and executable code. It is specifically designed to identify files and code embedded in firmware images. It uses the libmagic library, a unique library for recognizing the type of data in a computer file, so it is compatible with magic signatures created for the Unix file utility. Binwalk also includes a custom magic signature file that contains enhanced signatures for files commonly found in firmware images, such as compressed/archived files, firmware headers, Linux kernel, boot loader, file systems, etc.

Abilities of Binwalk:

- Finding and extracting interesting files/data from binary images,
- Finding and extracting raw compression streams,
- Identifying opcodes for a variety of architectures,
- Perform data entropy analysis,
- Diff any number of files.

SquashFS

SquashFS is a read-only compressed file system for GNU/Linux operating systems. SquashFS compresses files, inodes, and directories and supports block sizes up to 1 Mebibyte for better compression. It is accessed via a kernel module as a virtual file system. All files to be stored are packed into a file container similar to a compressed archive. Accesses are decompressed at runtime. With this particular behavior, the file system allows live systems or applications where only a small storage capacity is available. This makes it particularly suitable for use in embedded systems such as routers.

Analysis Methodology

This section will first discuss how the examined routers were selected and then explain how the examination took place and which options were selected for the examination.

Selection Procedure

In order to achieve a representative result, the examined routers were selected according to the following criteria. First, all of the three examined routers are from the manufacturer TP-Link in order to be able to compare them with each other. All three routers are also priced in the low budget range (under 20 Euros). All three routers are currently available in online stores and are sold in large quantities and purchased with little effort. To limit the availability of the investigated devices to one location, an international e-commerce provider was chosen. Since the company Amazon enjoys great sales nationally and internationally, the search for suitable models for the investigation was conducted here.

The first model chosen here was the TL-WR841N router (cf. 1). If one enters the search term "router" into the search bar at the e-commerce company Amazon, this model is the first one that is displayed in the low-budget range. It is also advertised with the attribute "Amazon's Choice" and has been voted the price-performance winner by Amazon's partner publishers. There are also more than 50,000 buyer reviews for this model, which suggests that this router can be found in many households.

The second model is the TP-Link Router TL-WR820N (cf. 2). This also lies in the low price segment and is very well rated by Amazon. Both models mentioned so far were provided as hardware for the investigation. They were selected in order to be able to provide a direct comparison between two TP-Link routers of almost identical pricing in terms of their security features.

The third router model selected for the investigation is the TP-Link Router TL-WR940N (cf. 3). This device was not provided as hardware. Only the corresponding software was downloaded and analyzed to show that despite the absence of the physical device, a security analysis of the firmware is also possible, and any weaknesses found could be exploited.

Investigation Procedures

To determine whether home network routers in a distributed attack can also be analyzed for vulnerabilities on a massive scale, it was examined whether it is possible to gain access to the firmware of a previously selected router model. This resulted in two possible approaches to examine the selected routers:

In the first test procedure, it should be found out to what extent a router present in hardware can be examined for security vulnerabilities. In the investigation, it was of particular interest how easy it is to find an interface or access the software via a weakness in the interface. For this purpose, the routers should be dismantled in the first step, whereby attention should be paid to how the respective router was protected against inappropriate access. The second step was to identify possible interfaces. After successfully identifying an interface, an attempt should be made to establish a connection via this same interface. If a connection could be established, it should be checked if it was possible to access a command line via this interface. After that, the router was to be put into operation, and the interface was to be checked for possible security issues. If there were any weak points in the interface, it was necessary to check whether it was possible to access the respective router's software. Finally, the

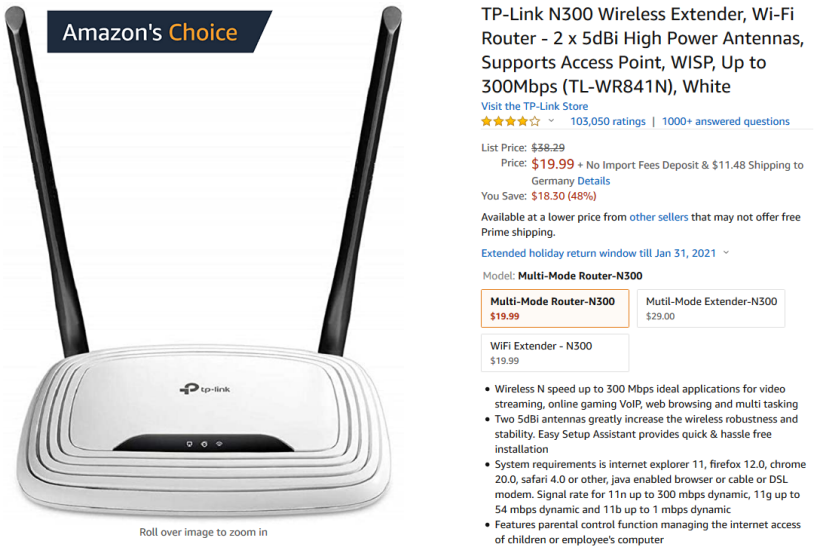


Figure 1. *Amazon Listing of TP-Link TL-WR841N Router*

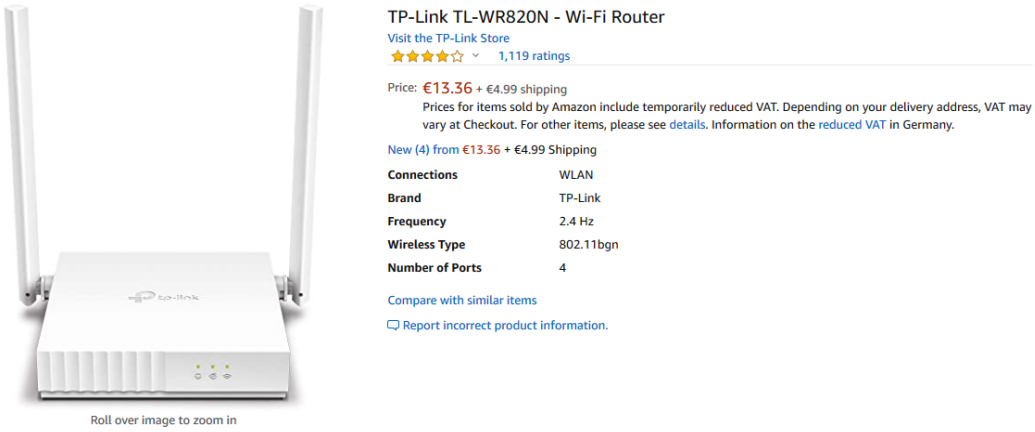


Figure 2. *Amazon Listing of TP-Link TL-WR820N Router*

software of the router had to be checked for known vulnerabilities.

The second test method was mainly to determine how easy it is to get access to firmware from selected devices. Furthermore, it was necessary to determine whether the files found were complete firmware or whether only updates in the form of parts of the firmware or individual program versions could be found. Afterward, it was of particular interest to determine which form the found firmware was available and how far it could be examined. If it should be possible to examine the software because it was available in unencrypted form, for example, a hardware-like environment should be created to determine whether it is possible to simulate a hardware-like environment with the help of the found software. Afterward, the firmware should be examined for known security vulnerabilities.

Investigation of Selected Devices

After the routers had been selected and the investigation methods determined, the practical investigation could begin. The first method, the analysis using existing hardware, was started initially.

After the hardware was purchased, it was removed from its packaging and examined to see how it could be opened (cf. 4,5).

Here there were screwed cases and click bindings, which could be opened almost without tools. All cases were opened with the help of a spatula to avoid damage to the cases (cf. 6,7).

After the case was opened, the corresponding pins had to be identified. The connection scheme of Receiver (RX), Transmitter (TX), and Ground (Gnd) had to be identified (cf. 8).

The corresponding pins were now connected to the corresponding connectors on a USB to TTL adapter (cf. 9). It was essential to note that the serial interface (USB) power source was not sufficient to power the router. When using a laboratory power supply that supplies the router with power, it was necessary to pay attention to the mass balance between the power supply and interface; otherwise, unwanted and dangerous short circuits could occur.

If the correct pins were connected to the serial interface

Figure 3. *Amazon Listing of TP-Link TL-WR940N Router*

Figure 4. *TP-Link TL-WR841N Router*

Figure 5. *TP-Link TL-WR820N Router*

Figure 6. *Dismantling of the TP-Link TL-WR841N Router*

and then to the PC, data transmission could be achieved with the correct baud rate. The baud rate of the examined routers was 115200 baud. If one wants to determine the baud rate, there are two ways to do this. On the one hand, there are lists of frequently used, so-called well-known baud rates on the Internet. With these lists' help, one can determine the baud rate necessary for the device by trial and error. The present baud rate of 115200 baud is already very high. Another way of determining the correct baud rate is to measure with an oscilloscope. After determining the correct baud rate, communication via the connection interface between PC and router is successful. The routers examined had 8 data bits and one stop bit. There was no parity bit on the examined routers. After a data connection was successfully

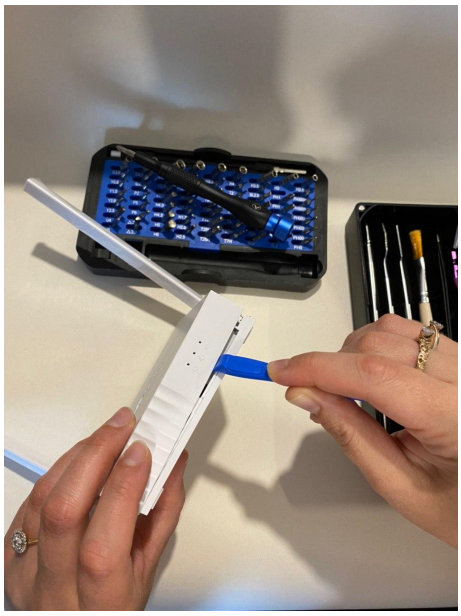


Figure 7. *Dismantling of the TP-Link TL-WR820N Router*

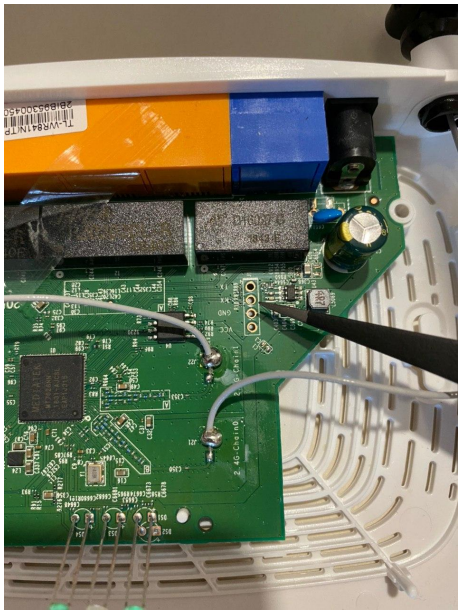


Figure 8. *Identification of the Interface of the TP-Link TL-WR841N Router*

established, the router could be accessed via a console on the PC. By entering a boot sequence, it was possible to obtain a root shell and gain control over the router. With this, it was possible to access the firmware, which could then be analyzed, and weak points could be investigated. This procedure's focus was to examine the existing software via a direct connection to the interface located on the hardware. The software's examination focused on determining the version numbers of the software used and comparing them with vulnerability databases. It was also examined to what extent certificates and private key files are hidden hard-coded in the software (cf. 10).

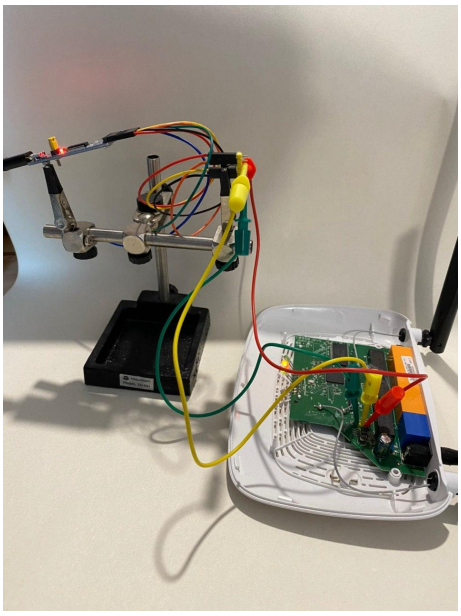


Figure 9. *Connection of the Interface of the TP-Link TL-WR841N Router*

For the second option of the safety investigation, it was unnecessary to have the selected router in hardware form. Using the router's model name, it was possible to search the Internet, especially the official TP-Link website, for the corresponding current firmware update (cf. 11).

For this case, special attention was also paid to the specified "release date". Also, attention was paid to hints which indicated whether vulnerabilities of the previous version had been closed with the respective version and whether this previous version was also available for download, which is not only an indicator for the fact that there are some versions of the firmware in circulation but also a clue for possible hackers who only had to search for vulnerable models with this information since the manufacturer himself disclosed the vulnerabilities. This information was surprisingly often provided with detailed information and CVE numbers (cf. 12).

For many of the examined routers, very recent updates were available. This led to the assumption that the update policy here should be of good quality. Once the latest firmware update was found, it could be downloaded to a PC and analyzed. This process was performed before unpacking the firmware to get first conclusions about packet structures etc (cf. 13,14).

With the tool Binwalk, which is quick and easy to use, the image file was now examined in more detail. Binwalk is generally used for analysis, reverse engineering, and extracting firmware images. With the commands "–signature" and "–term", which were executed on the firmware image, an overview of the memory address allocation became visible. For example, a boot loader and an LZMA file with a Squashfs file system were displayed. A file with the file extension LZMA is an LZMA compressed file. The suffix stands for Lempel-Ziv-Markov chain algorithm, and the files are mainly seen on Unix-based operating systems. LZMA files are similar to other compression algorithms like ZIP, which compress data to save space. However, it is known that LZMA compression provides faster decompression times than

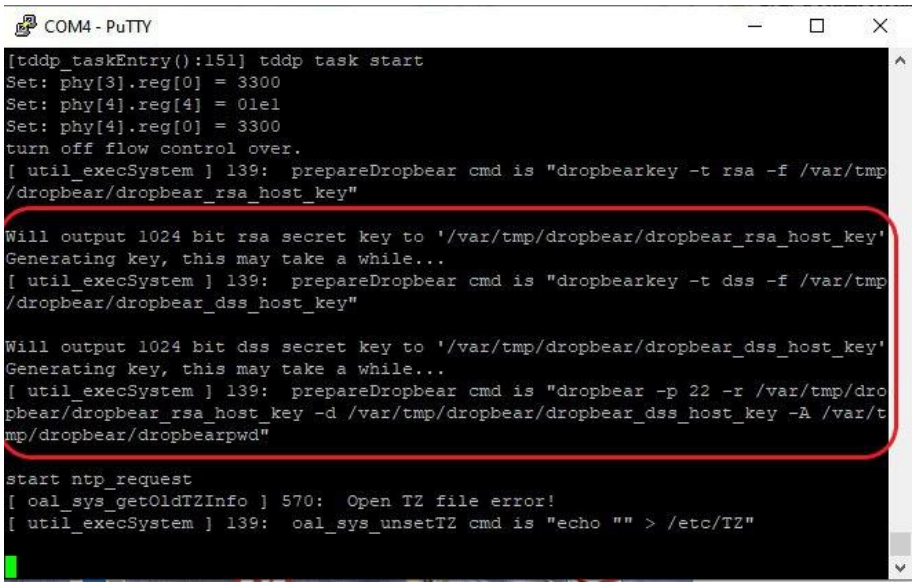


Figure 10. *Established Connection to the Interface of the TP-Link TL-WR841N Router and Information about Hard-Coded Key-Files*

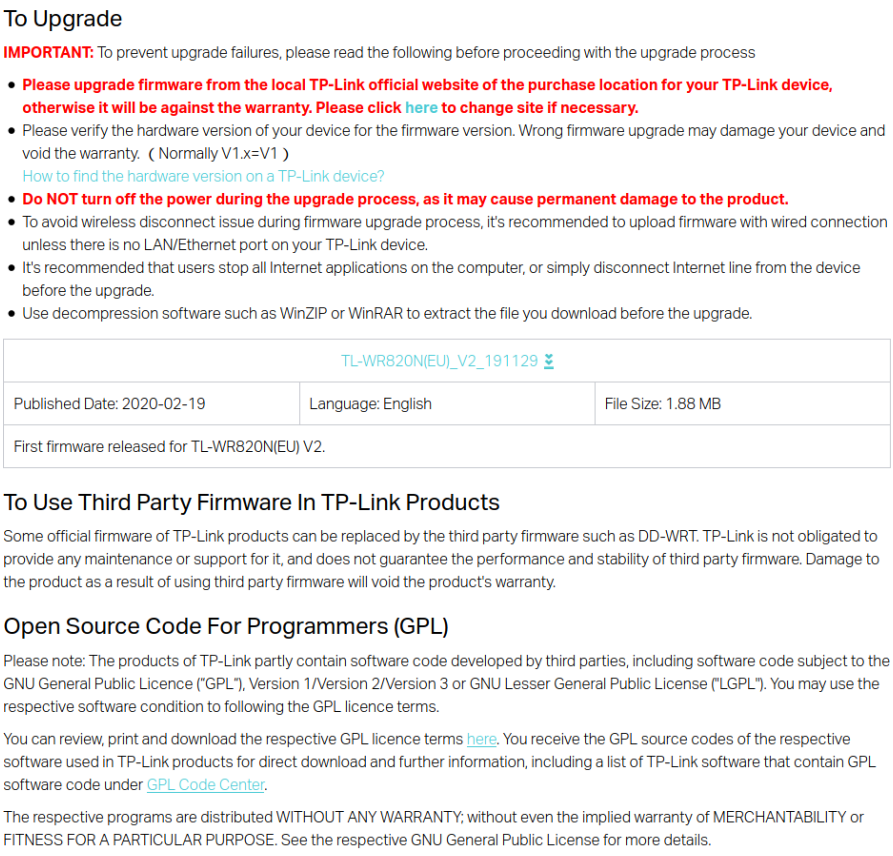


Figure 11. *Firmware Update and Upgrade Instructions for the TP-Link TL-WR820N Router*

other algorithms. This allocation of memory addresses already revealed much about the existing operating system. These steps have already shown that the operating system can vary greatly from model to model (cf. 15,16).

After this initial analysis, the firmware was unpacked (cf. 17).

However, to perform comprehensive analyses, the router's hardware environment had to be imitated. This was achieved by

Firmware

A firmware update can resolve issues that the previous firmware version may have and improve its current performance.

To Upgrade

IMPORTANT: To prevent upgrade failures, please read the following before proceeding with the upgrade process

- **Please upgrade firmware from the local TP-Link official website of the purchase location for your TP-Link device, otherwise it will be against the warranty. Please click here to change site if necessary.**
- Please verify the hardware version of your device for the firmware version. Wrong firmware upgrade may damage your device and void the warranty. (Normally V1.x=V1)
  How to find the hardware version on a TP-Link device?
- **Do NOT turn off the power during the upgrade process, as it may cause permanent damage to the product.**
- To avoid wireless disconnect issue during firmware upgrade process, it's recommended to upload firmware with wired connection unless there is no LAN/Ethernet port on your TP-Link device.
- It's recommended that users stop all Internet applications on the computer, or simply disconnect Internet line from the device before the upgrade.
- Use decompression software such as WinZIP or WinRAR to extract the file you download before the upgrade.

TL-WR940N(EU)_V6_200316		
Published Date: 2020-04-28	Language: English	File Size: 4.42 MB

New Features/Enhancement:
1. Optimized the wireless stability on RE mode.
2. Added the support for https.
3. Added support for reboot schedule.
4. Optimized the security and change the login mode.

Bug Fixes:
1. Fixed CVE-2020-8597.
2. Fixed CVE-2020-8423_84_V10.

Notes:
1. For TL-WR940N(EU) V6.
2. As we have added new functions in this version of firmware, once you have upgraded to this firmware, router will lose the old configuration.

Figure 12. *Firmware Update, Security Fixes with CVE Information and Upgrade Instructions for the TP-Link TL-WR940N Router*

```
┌─[~/Downloads/router-paper/investigation]─[schwarz@x1c6]─[0]─[10267]
└─[:)] % wget https://static.tp-link.com/2018/201804/20180403/TL-WR841N\(EU\)_V14_180319.zip
--2020-07-10 20:53:08--  https://static.tp-link.com/2018/201804/20180403/TL-WR841N(EU)_V14_180319.zip
CA-Zertifikat »/etc/ssl/certs/ca-certificates.crt« wurde geladen
Auflösen des Hostnamens static.tp-link.com (static.tp-link.com)… 99.84.156.85, 99.84.156.88, 99.84.156.100, ...
Verbindungsaufbau zu static.tp-link.com (static.tp-link.com)|99.84.156.85|:443 … verbunden.
HTTP-Anforderung gesendet, auf Antwort wird gewartet … 200 OK
Länge: 4334488 (4,1M) [application/zip]
Wird in »TL-WR841N(EU)_V14_180319.zip« gespeichert.

TL-WR841N(EU)_V14_180319.zip                      100%[=============================================================================================================>]   4,13M  3,94MB/s    in 1,0s

2020-07-10 20:53:10 (3,94 MB/s) - »TL-WR841N(EU)_V14_180319.zip« gespeichert [4334488/4334488]
```

Figure 13. *Download of an Update File for the TP-Link TL-WR841N Router*

```
┌─[~/Downloads/router-paper/investigation]─[schwarz@x1c6]─[0]─[10270]
└─[:)] % ls
'TL-WR841N(EU)_V14_180319.zip'
┌─[~/Downloads/router-paper/investigation]─[schwarz@x1c6]─[0]─[10271]
└─[:)] % unzip TL-WR841N\(EU\)_V14_180319.zip
Archive:  TL-WR841N(EU)_V14_180319.zip
  inflating: TL-WR841Nv14_EU_0.9.1_4.16_up_boot[180319-rel57291].bin
  inflating: GPL License Terms.pdf
  inflating: How to upgrade TP-LINK Wireless  N Router.pdf
┌─[~/Downloads/router-paper/investigation]─[schwarz@x1c6]─[0]─[10272]
└─[:)] % ls
 GPL License Terms.pdf  'How to upgrade TP-LINK Wireless  N Router.pdf'  'TL-WR841N(EU)_V14_180319.zip'  'TL-WR841Nv14_EU_0.9.1_4.16_up_boot[180319-rel57291].bin'
```

Figure 14. *Extraction of an Update File for the TP-Link TL-WR841N Router*

```
┌─[~/Downloads/router-paper/investigation]─[schwarz@x1c6]─[0]─[10273]
└─[:)] % binwalk --signature --term TL-WR841Nv14_EU_0.9.1_4.16_up_boot\[180319-rel57291\].bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
53952         0xD2C0          U-Boot version string, "U-Boot 1.1.3 (Mar 19 2018 - 15:36:42)"
66560         0x10400         LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 2986732 bytes
1049088       0x100200        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2966369 bytes, 611 inodes, blocksize: 262144 bytes, created: 2018-03-19 07:55:53
```

Figure 15. *Binwalk Output for the Update File of the TP-Link TL-WR841N Router*

emulating the hardware environment with Qemu. Subsequently, a comprehensive security analysis of the firmware could be car-

```
┌─[~/Downloads/router-paper/investigation]─[schwarz@x1c6]─[0]─[10285]
└─[:)] % binwalk --signature --term -v wr940nv6_eu_3_20_1_up_boot\(200316\).bin

Scan Time:     2020-07-10 21:00:19
Target File:   /home/schwarz/Downloads/router-paper/investigation/wr940nv6_eu_3_20_1_up_boot(200316).bin
MD5 Checksum:  d7dd601b9fb33739236cec85e9ac055f
Signatures:    391

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------------------------------
0             0x0             TP-Link firmware header, firmware version: 0.-6164.3, image version: "",
                              product ID: 0x0, product version: 155189254, kernel load address: 0x0,
                              kernel entry point: 0x80002000, kernel offset: 4063744, kernel length:
                              512, rootfs offset: 866618, rootfs length: 917504, bootloader offset:
                              3014656, bootloader length: 0
15552         0x3CC0          U-Boot version string, "U-Boot 1.1.4 (Mar 16 2020 - 09:26:38)"
15600         0x3CF0          CRC32 polynomial table, big endian
16900         0x4204          uImage header, header size: 64 bytes, header CRC: 0xCB6027D7, created:
                              2020-03-16 01:26:38, image size: 42920 bytes, Data Address: 0x80010000,
                              Entry Point: 0x80010000, data CRC: 0x11F3A251, OS: Linux, CPU: MIPS,
                              image type: Firmware Image, compression type: lzma, image name: "u-boot
                              image"
16964         0x4244          LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes,
                              uncompressed size: 114016 bytes
131584        0x20200         TP-Link firmware header, firmware version: 0.0.3, image version: "",
                              product ID: 0x0, product version: 155189254, kernel load address: 0x0,
                              kernel entry point: 0x80002000, kernel offset: 3932160, kernel length:
                              512, rootfs offset: 866618, rootfs length: 917504, bootloader offset:
                              3014656, bootloader length: 0
132096        0x20400         LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes,
                              uncompressed size: 2496348 bytes
333162        0x5156A         MPEG transport stream data
1049088       0x100200        Squashfs filesystem, little endian, version 4.0, compression:lzma, size:
                              2989254 bytes, 690 inodes, blocksize: 262144 bytes, created: 2020-03-16
                              01:33:58
```

Figure 16. *Binwalk Output for the Update File of the TP-Link TL-WR940N Router*

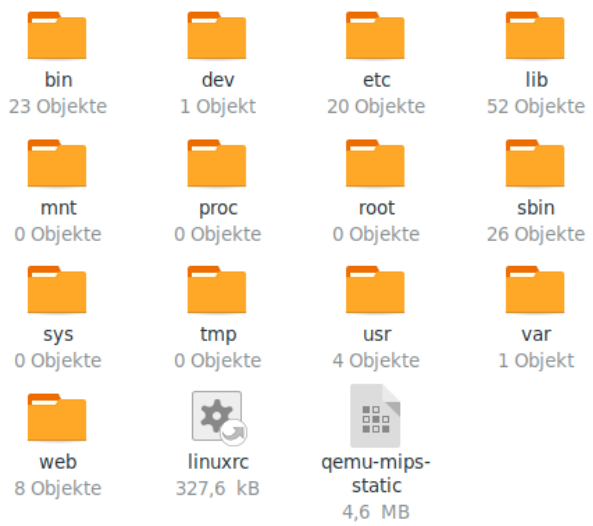


Figure 17. *Unpacked Firmware of the TP-Link TL-WR940N Router*

ried out, and weaknesses and vulnerabilities in the software could be searched for. As in the first method, it was possible to design access as if the hardware existed, and so here, too version numbers were taken into account, and the extent to which private keys and certificates can be found in the code was examined. This is a particular gap here because these keys and certificates can be extracted automatically (cf. 18).

Summary and Outlook

This paper shows that all of the routers examined have serious weaknesses, which often lead to the fact that they can be taken over and remotely controlled by others. They thus represent a significant weakness for the home network and the integrity of the Internet in general and for all the smart home devices in it that are supposed to secure it. There are no uniform standards regarding manufacturers' update policies for different router models, making it impossible to predict whether a router is secure and whether it is advisable to buy it. This research has also shown that even the fixing of current vulnerabilities is no guarantee that older vulnerabilities have been fixed. Current updates are, therefore, no guarantee for the security of a device. To make matters worse, manufacturers make it difficult, if not impossible, for users to modify the firmware to meet their own security standards. Open source solutions like OpenWrt are difficult to integrate because the law requires that only the manufacturers' firmware can run on the devices. Often the devices are also designed so that due to extreme savings, no current alternative firmware fits on the devices, which severely limits the use of these devices at the latest after the support time has expired. A short test found that many TP-Link routers with challenging numbers could be found in the Shodan search engine. The manufacturer has also made the vulnerabilities of old firmware visible to everyone on its update pages. So it may be possible that due to the openly accessible information in Shodan and on the manufacturer's site, devices can be hacked without any analysis. Future work could build on this work's results and examine models from other manufacturers and higher price segments. For example, whether a higher price also offers a

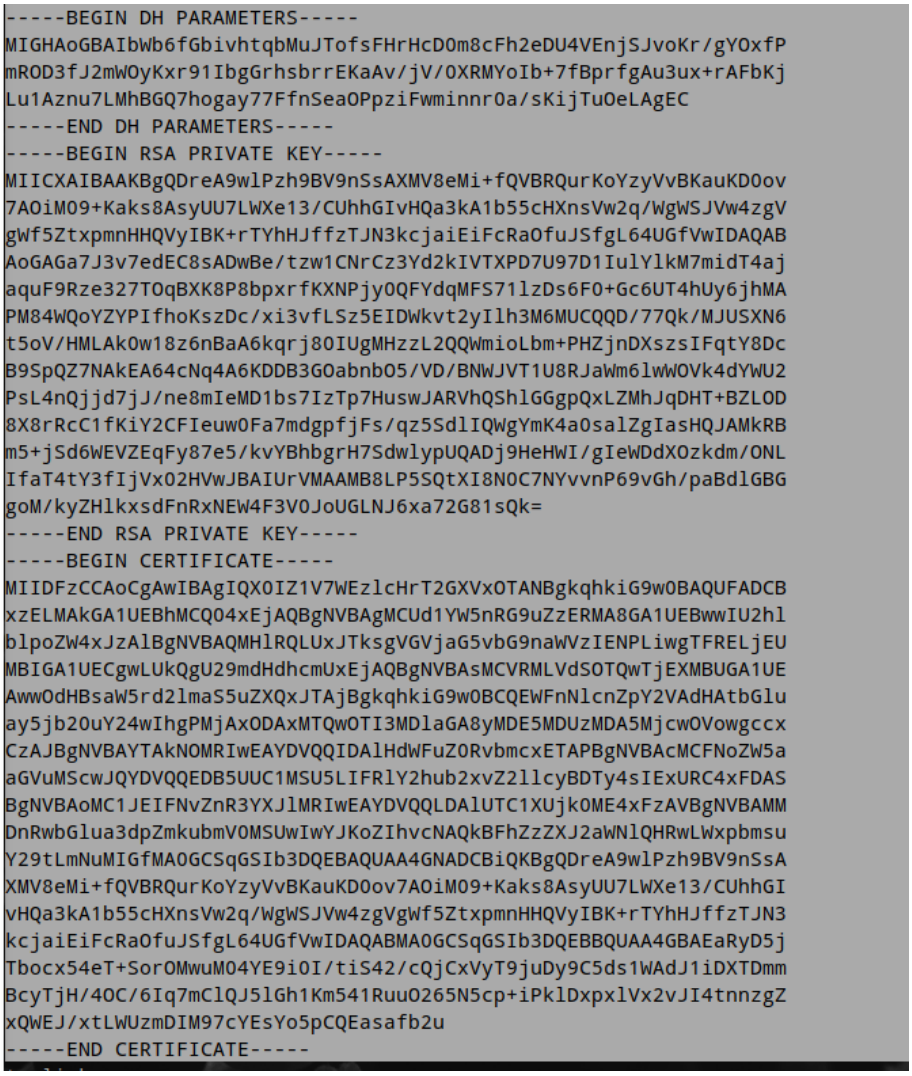


Figure 18. *Hardcoded and in Software Hidden DH Parameters, Private Key and Certificate for the TL-WR820N Router*

higher level of security would have to be clarified.

References

[1] Ziring: Router Security Configuration Guide Supplement - Security for IPv6 Routers. CreateSpace Independent Publishing Platform 2015

[2] Schudelo, G.; D. Smith: Router Security Strategies: Securing IP Network Traffic Planes. Cisco Press 2007

[3] Visoottiviseth, V.; Jutadhammakorn, P.; Pongchanchai, N.; Kosolyudhthasarn, P.: Firmaster Analysis Tool for Home Router Firmware. *Proc. 2018 IEEE 15th International Joint Conference on Computer Science and Software Engineering (JCSSE)*

[4] Teng, C.-C.; Gong, J.-W.; Wang, Y.-S.; Chuang, C.-P.; Chen, M.-C.: Firmware over the air for home cybersecurity in the Internet of Things. Proc. 2017 IEEE APNOMS, pp. 123-128.

[5] Dua, A.; Tyagi, V.; Patel, N. D.; Methre, B. M.: IISR: A Secure Router for IoT Networks. Proc. IEEE 2019 4th International Conference on Information Systems and Computer Networks (ISCON), GLA University, Mathura, UP, India. Nov 21-22, 2019, pp. 636-643.

[6] Kasemsuwan, P.; Visoottiviseth, V.: OSV OSPF vulnerability checking tool. IEEE 2017

[7] Adithyan, A.; Nagendran, K.; Chethana, R.; Gokul Pandy, D.; Gowri Prashanth, K.: Reverse Engineering and Backdooring Router Firmwares. Proc. IEEE 2020 6th Internat. COnf. on Advanced Computing & Communication Systems (ICACCS), pp. 189-193

[8] "Vulnerability assessment," [Online]. Available: `https://en.wikipedia.org/wiki/Vulnerability_assessment` (last access: February 21, 2021).

[9] Khandelwal, S.: "World's largest 1 Tbsp. DDoS Attack launched from 152,000 hacked Smart Devices," The Hacker News, [Online]. Available: `https://thehackernews.com/2016/09/ddos-attack-iot.html` (last access: February 21, 2021).

[10] OWASP IoT Top 10 [Online]. Available: `https:`

//owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf (last access: February 21, 2021).
[11] von Westernhagen, O.: Abgekündigte Router-Modelle von D-Link: Kein Update für Firmware-Schwachstelle, heise online 2019, https://www.heise.de/security/meldung/Abgekuendigte-Router-Modelle-von-D-Link-Kein-Update-fuer-Firmware-Schwachstelle-4548695.html, (October 08, 2019), (last access: February 21, 2021).
[12] Schmidt, J.: Kritische 0day-Lücke in 79 Netgear-Router-Modellen, heise online, https://www.heise.de/security/meldung/Kritische-0day-Luecke-in-79-Netgear-Router-Modellen-4789814.html, (June 19, 2020).
[13] Dhanjani, N.; Thiele, N.: *IoT-Hacking: Sicherheitslücken im Internet der Dinge erkennen und schließen.* Heidelberg: dpunkt.verlag 2016.
[14] Schirrmacher, D.: Zero-Day-Lücke in Smart-Home-Router SR20 von TP-Link, heise online, https://www.heise.de/security/meldung/Zero-Day-Luecke-in-Smart-Home-Router-SR20-von-TP-Link-4356942.html. (last access: February 21, 2021).
[15] Funkanlagengesetz (FuAG), Bundesgesetzblatt, Bundesanzeiger Verlag. Bonn (03. 07.2017).
[16] TP-Link, Company profile TP-Link, https://www.tp-link.com/de/about-us/corporate-profile (last access: February 21, 2021).
[17] Gierow, H.: Router-Botnetz mit 500.000 Geräten aufgedeckt, Golem online 2018, https://www.golem.de/news/vpnfilter-router-botnetz-mit-500-000-geraeten-aufgedeckt-1805-134557.html. (last access: February 21, 2021).
[18] Scherschel, F. A.: Alarmierender Fraunhofer-Test: Viele Home-Router unsicher, heise online 2019. https://www.heise.de/news/Keine-Ueberraschung-nach-Frauenhofer-Test-Viele-Home-Router-unsicher-4798342.html, (last access: February 21, 2021).
[19] Ray, A. K. and Bagwari, *IoT based Smart home: Security Aspects and security architecture*, 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT) 2020 pp.218-222

Author Biography

Franziska Schwarz is a M. Sc. student of Computer Science at Technische Hochschule Brandenburg (Germany). She received her B. Sc. in 2019 and is working as a scientific assistant in Technische Hochschule Brandenburg and is expected to complete her master's degree in 2021. Her research work is focused on IoT and Smart Home Security, Cybersecurity, and IT Security Management.

Klaus Schwarz received his B. Sc. and M.Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2017 and 2020, respectively. His research interests include IoT and Smart Home Security, OSINT, Mechatronics, Sensorics, Embedded Systems, Artificial Intelligence, and Cloud Security. As a faculty member, he is developing a graduate program in Applied Mechatronic Systems focusing on Artificial Intelligence at SRH Berlin University of Applied Sciences.

Daniel Fuchs received his B. Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2018. He is finishing his Master Thesis in 2021 and his research interests include IoT and Embedded Systems as well as Cloud Security.

Reiner Creutzburg is a Retired Professor for Applied Computer Science at the Technische Hochschule Brandenburg in Brandenburg, Germany. Since 2019 he is a Professor of IT Security at the SRH Berlin University of Applied Sciences, Berlin School of Technology. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Devices (MOBMU) Conference at the Electronic Imaging conferences since 2005. In 2019, he was elected a member of the Leibniz Society of Sciences to Berlin e.V. His research interest is focused on Cybersecurity, Digital Forensics, Open Source Intelligence (OSINT), Multimedia Signal Processing, eLearning, Parallel Memory Architectures, and Modern Digital Media and Imaging Applications.

David Akopian is a Full Professor and Associate Dean of Research in the Department of Electrical and Computer Engineering at The University of Texas San Antonio (UTSA). His research interest is focused on Spread Spectrum Communications, Positioning Systems and Healthcare. He presides as a director over the Software Communications and Navigation Systems Lab (SCNS) include wireless sensing, human activity data collection, localization technologies and supporting mobile applications.

Appendix 1: The results of the analysis in summary

Router	CVE/Vulnerability
TL-WR820N	Root CA, Private Key and Public Key are unencrypted in the file system of the publicly accessible update file
TL-WR841N, TL-WR940N	CVE-2018-11714 This issue is caused by improper session handling on the /cgi/ folder or a /cgi file. If an attacker sends a header 7of "Referer: http://192.168.0.1/mainFrame.htm" then no authentication is required for any action. CVE-2018-1257 The Ping and Traceroute features allow authenticated blind Command Injection. CVE-2018-12576 Devices allow clickjacking. CVE-2018-12575 All actions in the web interface are affected by bypass of authentication via an HTTP request. CVE-2018-12574 CSRF exists for all actions in the web interface. CVE-2012-6316 Multiple cross-site scripting (XSS) vulnerabilities allow remote administrators to inject arbitrary web script or HTML via the (1) username or (2) pwd parameter to NoipDdnsRpm.htm CVE-2012-6276 Directory traversal vulnerability in the web-based management interface allows remote attackers to read arbitrary files via the URL parameter. CVE-2012-5687 Directory traversal vulnerability in the web-based management feature allows remote attackers to read arbitrary files via a ".." (dot dot) in the PATH_INFO to the help/ URI.

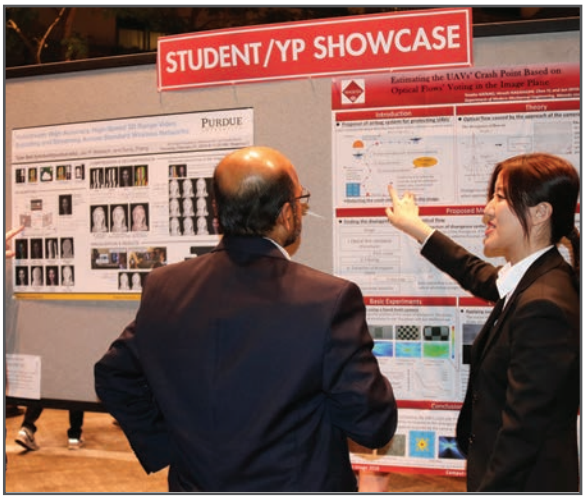
JOIN US AT THE NEXT EI!

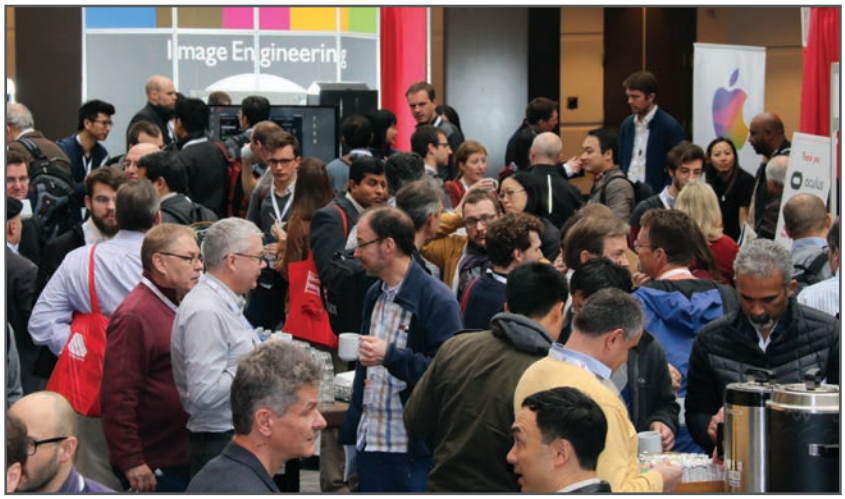
IS&T International Symposium on

Electronic Imaging

SCIENCE AND TECHNOLOGY

Imaging across applications . . . Where industry and academia meet!





• SHORT COURSES • EXHIBITS • DEMONSTRATION SESSION • PLENARY TALKS •
• INTERACTIVE PAPER SESSION • SPECIAL EVENTS • TECHNICAL SESSIONS •

www.electronicimaging.org

IS&T
imaging.org