CVE-2020-24297 and CVE-2020-28005: Vulnerabilities in TP-Link's TL-WPA4220

2020-11-18 | *3 minutes* | #CVE-2020-24297 #CVE-2020-28005 #embedded #TP-Link

In this post, I'm going to describe some vulnerabilities that I found a while ago, affecting the HTTP server of TP-Link's Powerline Adapter/WiFi Extender TL-WPA4220 (hardware versions 2, 3, and 4). These flaws are **two command injection vulnerabilities** that can grant an attacker root access to the device (CVE-2020-24297), as well as **a stack-based buffer overflow vulnerability** that can be used to crash the `http` service (CVE-2020-28005).

These flaws can be exploited by a remote authenticated attacker that is connected to the LAN, or that has access to the web management interface in the uncommon situation that it is exposed to the internet. As the default password for the web interface is easily guessable (yes, it's `admin`), in most cases this means that anyone connected to the LAN can take advantage of them.

After disclosing these flaws to TP-Link, they have been patched in the latest firmware version `TL-WPA4220(EU)_V4_201023` (you can get it here), which corresponds to hardware version 4. For hardware versions 2 and 3 no patch has been published to the moment, so all versions are still vulnerable.

For a thorough explanation of how I found these vulnerabilities, see the *Hacking the TL-WPA4220* series:

- Hacking the TL-WPA4220, Part 1: Laying the Ground
- Hacking the TL-WPA4220, Part 2: The Command Injections
- Hacking the TL-WPA4220, Part 3: Talking to the Server
- Hacking the TL-WPA4220, Part 4: The Buffer Overflow

CVE-2020-24297

The command injection vulnerabilities exist in the endpoint `/admin/powerline`, when the `form` parameter is set to `plc_add` or `plc_device`, and malicious POST data is passed. The existing flaw is caused by the insufficient validation or sanitization of the POST parameters `devicePwd` and `key` respectively. See CVE page here.

Since the HTTP server is running as `root`, these vulnerabilities can be used to take full control of the device.

A PoC for this vulnerability can be found here.

CVE-2020-28005

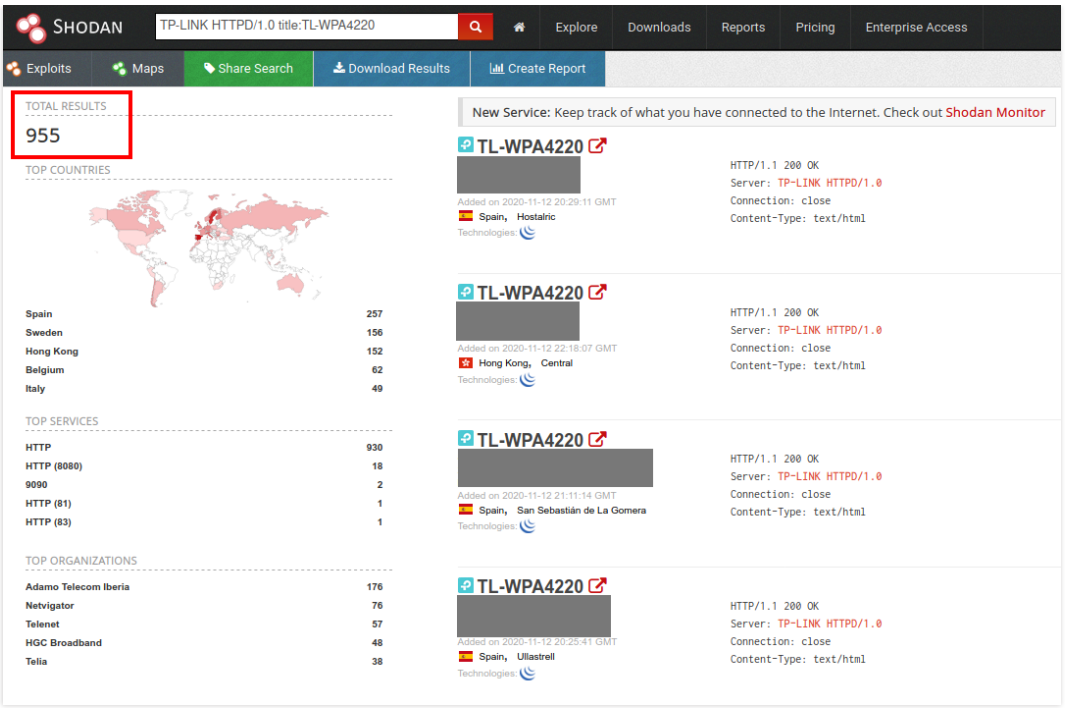
The stack-based buffer overflow exists in the endpoint `/admin/syslog`, when the `form` parameter is set to `filter`, and malicious POST data is passed. The existing flaw is caused by the unexisting validation of the length of the POST parameter `type`. See CVE page here.

Since partial Address Space Layout Randomization (ASLR) is enabled on the device, this vulnerability alone can't be used to achieve remote code execution. However, it can be used to crash the HTTP service.

A PoC for this vulnerability can be found here.

Exposed Devices

As mentioned above, to exploit these vulnerabilities an attacker has to be connected to the LAN to be able to access the web management interface. However, a quick Shodan search reveals that a total of **995 TL-WPA4220 devices have their web management interface exposed to the internet**, and are therefore potentially exploitable by remote attackers:



Of course, to be exploitable, these devices need to have a vulnerable firmware version, and the default (or a guessable) password, so most probably not all of these devices can be exploited.

Recommendations

- **Change the default password** of the web management interface to a non-guessable, secure one.
- If your TP-WPA4220 has hardware version 4, **upgrade the firmware** with the latest release (see the vendor's page).

Disclosure Timeline

- **2020/07/20** - First command injection vulnerability reported to the vendor
- **2020/08/04** - Vulnerability confirmed by the vendor. Additional command injection and buffer overflow vulnerabilities reported to the vendor
- **2020/10/27** - Firmware upgrade shared by the vendor
- **2020/10/29** - Confirmation to the vendor that the reported vulnerabilities had been fixed in the upgraded firmware
- **2020/11/12** - Firmware upgrade published
- **2020/11/18** - Publication of CVE-2020-24297 and CVE-2020-28005 by MITRE

EDIT:

- **2020/12/18** - At some point before this date, TP-Link removed the firmware upgrade from their site (for reasons unknown to me). I asked them to put the upgrade back as soon as possible
- **2021/01/13** - Firmware upgrade is republished