# Netgear Does Not Need Customers

Firmware Updates Are Overrated

Onkobu Tanaake

2020-09-21T10:00:00

Netgear sells many different types of network hardware. Like all modern complex products their switches, routers and access points require firmware updates. Nowadays this isn't something for the average customer without a separate service contract.

I own two Netgear switches, bought in 2018. One is a five port GS105v3E and the second is a GS108v3E. They serve a simple purpose: switch multiple computers at home onto a single gateway. From time to time I run maintenance tasks for all my hardware. For example I read through the change logs and comb out security issues. Sometimes it is necessary to do a firmware upgrade to fix a bunch of issues.

The 5-port-model was done quite fast. I got the firmware image from the Netgear page, pushed the binary through the web interface onto the switch and restarted it. I moved on the 8-port-model and spent 2 hours for a task that should last not longer than 10 minutes.

During the update process I stumbled accross multiple (Netgear-) community articles, blog posts and forum entries. They all failed to update the firmware since 2015 for various reasons. Today is September 2020 and Netgear didn't take the time to fix the issues. It starts with putting the switch into so called loader mode. The regular web user interface is turned off and a minimal file-upload form appears.

I uploaded the firmware image and nothing happened for about 2 minutes. Underneath the progress bar dialog I saw a connection reset-message issued by the browser. So I restarted the entire process. I did this more than 10 times in total. In addition I tried various reset methods and ended up with a switch that didn't return to the web UI anymore. Normally a reset to factory defaults or reboot from the loader mode brings back the web UI.

So all I could do was find a Windows computer – I only run Linux – and try an update from there. The first attempt with the same binary was successful right away. I have absolutely no idea about the reason. It is a simple file upload and Netgear managed to fail the implementation and turn a lot of switches into unconfigurable bricks unless you have Windows and time to spare or a need for a configurable switch.

What I tried:

- Disable compression when uploading, accept header
- use Chrome or Midori or Links (on Linux)
- replay the POST request with cURL, yields an empty response

- Disable caching

What I assume:

- The progress bar is not coupled to anything upload-related, it is an unnecessary piece of JavaScript doing image manipulation
- It is not triggered by the User-Agent, modified it to match the Windows-version, left it out entirely, didn't change anything
- There is structured memory for the configuration, after multiple hard resets and a successful update the previous configuration, incl. a complex password, was suddenly restored
- Restoring previously saved configurations does not work, Web UI complains about a format error, maybe the same upload issue

And as a sidenote: Netgear publishes security issues but the description is abstract nonsense. It neither contains a clear description what is affected, nor how the issue is exploited and how it was fixed. I have absolutely no idea, how to detect an attack nor how to mitigate such attacks on another network layer. And how bad can a *Sensitive Information Disclosure* be for a device that has a password based login without any TLS?

- Community article 1 [https://community.netgear.com/t5/Smart-Plus-and-Smart-Pro-Managed/Web-firmware-upgrade-for-GS108Ev3-failing/m-p/997816/highlight/true]
- Community Article 2 [https://community.netgear.com/t5/Smart-Plus-and-Smart-Pro-Managed/GS108Ev3-firmware-upgrade-failed-and-cannot-factory-reset/m-p/1563115/highlight/true]
- Blog Post [https://andidittrich.com/2018/07/netgear-gs108ev3-firmware-upgrade-failed.html]
- Computerbase Forum [https://www.computerbase.de/forum/threads/netgear-gs108ev3-switch-firmwareupdate-klappt-nicht-wieso.1514671/]
- Sensitive Information Disclosure on Some Switches, PSV-2018-0612 [https://kb.netgear.com/000061481/Security-Advisory-for-Sensitive-Information-Disclosure-on-Some-Switches-PSV-2018-0612]
- Missing Function Level Access Control on Some Switches, PSV-2018-0542 [https://kb.netgear.com/000061463/Security-Advisory-for-Missing-Function-Level-Access-Control-on-Some-Switches-PSV-2018-0542]
- Tweet Don't buy Netgear [https://twitter.com/lindworm/status/1307678495158530053] – Added Oct. 23rd, 2020