idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE
Silke Wiesemann

30.11.2022
http://idw-online.de/de/news805785

Forschungsergebnisse, Wissenschaftliche Publikationen
Informationstechnik
überregional

Fraunhofer FKIE publishes Home Router Security Report 2022

They are in use everywhere but are yet rarely in the spotlight: home routers. At the latest since working from home has become a prevalent model in the Corona pandemic, not only private but also professional network traffic crosses these devices. Thus, there are plenty of reasons for scientists at the Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE to take another look at the security of home routers after 2020. Their conclusion: the trend shows improvements compared to 2020, but there is still some work to be done.

Scientists of the FKIE department “Cyber Analysis & Defense” analyzed 122 router models that were on the market as of 31 March 2022. For corpus construction, they selected seven thirdparty vendors who sell their devices in Europe, but also internationally. Similar to the Home Router Security Report 2020, the security experts downloaded the freely available software of all 122 examined models, the so-called firmware, and analyzed it for the implementation of broadly recognized security best practices.

"The goal of this report is to raise awareness of the fact that well-established security practices must also be taken into account for such pivotal network devices as home routers. On the one hand, they can be directly accessed from the internet and on the other hand, they serve as gatekeepers for other devices in the local network," says research group leader Johannes vom Dorp. FKIE scientist René Helmke adds: "We share our results with the vendors before publishing the report. Our aim is to point out potential issues so that they can be remedied, thus improving the safety of the devices in the long term."

Two-step methodology

The analysis was done in two steps: First, the firmware was automatically unpacked and evaluated according to predefined research questions. For example, when did the device last receive an update? Are there any publicly known security issues in the operating system? Are there any hard-coded login credentials? The scientists carried out this automated analysis using the open source "Firmware Analysis and Comparison Tool" (FACT) developed at Fraunhofer FKIE.
Already in the first step, a fully automated analysis, new methods were added to further improve result reliability compared to the 2020 report. As for the second step, which focuses on the evaluation of potential vulnerabilities in the operating system, the scientists developed and published a novel heuristic for the 2022 report. This provides further insights into result interpretation of the previous analysis and reduces false-positive rates.

Results

The analysis showed that the seven vendors address device security very differently: There were devices with only a few potential security issues, but others indicated a clear need for improvement regarding all investigated research questions. Patches, i.e., software updates that may also address security issues, are applied in a timelier manner and the operating system versions are updated at somewhat shorter intervals in comparison to 2020 – although not yet to a sufficient extent in the opinion of the security experts. Also interesting is a clear decline in hard-coded login data. However, the security experts identify a greater security problem in easily guessable passwords, the number of which has not changed significantly. In addition, available protection measures for binary executable files, so-called "binary hardening" methods, are not used consistently in many cases. Finally, the Linux versions used for routers were compared with a public database that documents known security vulnerabilities. The scientists then filtered the results using a new method in order to consider only those potential security vulnerabilities that may also be applicable to the routers in question. Helmke clarifies: "Due to this modified heuristic the results of 2020 and 2022 are not comparable in this regard."

Recommendations to router vendors

Therefore, the scientists' recommendation to vendors is to replace operating system versions that no longer receive security updates more frequently. It is also beneficial to modernize build chains in order to activate security-relevant compiler features. All hard-coded credentials should be checked for their necessity. And finally, passwords that are not easy to crack should be used. "Some of these changes are easy to implement, but can increase security considerably," summarizes vom Dorp.

wissenschaftliche Ansprechpartner:

Fraunhofer FKIE
Department "Cyber Analysis & Defense"
Prof. Dr. Elmar Padilla
Mail: presse@fkie.fraunhofer.de

Originalpublikation:

https://www.fkie.fraunhofer.de/en/press-releases/Home-Router1.html