Finding Zero-Day Vulnerabilities

Fletcher Davis, Peyton Edmondson, Austin Griffith, Austin Harlow, Clifford Krey
Department of Cybersecurity Engineering, George Mason University

Objectives

Assess the attack surface and perform vulnerability research on the embedded software system of the Huawei HG8245H router.

Help Sponsor better understand vulnerabilities in devices to aid in supply chain procurement risks.

Open-Source Tools

Kali Linux
Operating system used for our research, development, testing, and virtual exploitation environment.

Burp Suite
Analyze network protocols between router and client

Firmware Slap
Used on the router's firmware to find potential buffer overflow vulnerabilities

Huawei Forums
Download router firmware and discover super-admin credentials

Vulnerability Research

Open-Source Research
Our initial focus was understanding the HG8245h (right). Then metadata was gathered and used to perform a search. Huawei forums were especially helpful.

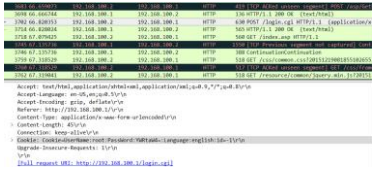
Firmware Extraction
In order to find software vulnerabilities on the router, we must obtain a copy of the firmware. Through the debug interfaces UART and JTAG, as well as through the vendor image repositories, we were able to obtain a binary image.

Firmware Analysis
Firmware was acquired online and pulled from device, Then the filesystem was extracted and examined using Binwalk. Lastly, Firmware Slap was used on the router's firmware /bin/ directory to find buffer overflows.

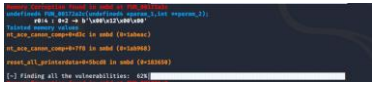
Hardware Analysis
Router was disassembled and internal components were photographed and documented. Data for chipsets was collected.

Software Analysis
List of software pre-installed on the router was cross referenced with known vulnerabilities for each software's specific version.

Penetration Testing
Used open-source tooling to analyze the web interface for web application vulnerabilities. Utilized tooling to fuzz UPnP input on the exposed UPnP port in an attempt to cause a crash.



Wireshark output of the wireless password disclosure vulnerability



Firmware Slap: Automated firmware analysis tool scanning firmware function for vulnerabilities

Results

Firmware Vulnerabilities
333 potential buffer overflows within the router's firmware could be exploited to allow an unauthorized access of memory.

Hardware Vulnerabilities
Exposed debug interfaces allow access to filesystem to extract device memory and firmware. Unencrypted firmware package. Lack of integrity and authenticity check allowed for the upload of malicious firmware that included a backdoor.

Web-Based Vulnerabilities
Wireless HTTP router credential sniffing vulnerability found a web cookie that contains unencrypted login credentials. Default super-admin credentials were found, contacting Huawei is required to change them.
Username: telecomadmin Password: admintelecom

Conclusion

Vulnerability research on the Huawei HG8245H router yielded numerous vulnerabilities and even more potential vulnerabilities

With additional time the workflow can be continued to reverse engineer the potential vulnerabilities found

The results of this research validate the United States Government's mistrust in Huawei

Workflow can be recreated on other devices to test their security

Acknowledgments

Our wonderful project would not have been possible without Professor Rock Sabetto for organizing this Capstone class, our mentor Dr. Powell for his guidance, Sasha Morgan for representing our sponsor Lockheed Martin, Dr. Jones and Dr. Winston for guidance on reverse engineering, and Chris Roberts for creating "Firmware Slap".

References

C. Roberts. "Firmware Slap." Github. https://github.com/ChrisTheCoolHut/Firmware_Slap (accessed April 5, 2020).
U.S. House. 115th Congress, 1st session. (2018, Apr. 13). *H.R.5515, John S. McCain National Defense Act for Fiscal Year 2019*. [Online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/5515/text
D. Burstein. "Huawei's Very Red World." Circle ID. http://www.circleid.com/posts/20190830_huaweis_very_red_world/ (accessed April 5, 2020).