Military-grade HW appliance penetration test

Retia, a.s.

Task

Auxilium Cyber Security was approached by RETIA to conduct a penetration test in order to determine the exposure of RETIA's device to targeted attacks by malicious users.

RETIA is a Czech company performing its own research and high quality manufacturing in the field of military electronics and recording systems with deliveries around the world. Considering the importance of security in military equipment, one of the critical requirements was to ensure the tested device met the implied level of cyber security.

Device tested by Auxilium was in still in the SW development phase during the penetration test. One of the key goals of the penetration test was to utilize the results for SW finalization in the device further strengthening its resiliency and security.

Solution

Based on our prior experience with hardware and automotive penetration testing, we offered to provide thorough security testing of the device. Due to the complex and customized nature of this device, testing had to be adapted and specialized for its needs. Testing of the device conducted in a manner that simulated malicious user scenarios and attacks which targeted the infrastructure and web application part of the device, with the phases of the testing being the following:

- Identify security risks and vulnerabilities on the Retia Data Diode administration web portal. The first part of testing was targeting the web portal of RETIA's device that was hosted in the device using several different technologies that are publicly available. The tests conducted to the target web portal was split in automated and manual testing, following industry standards and common web security issues (OWASP Top 10).
- Identify security risks and vulnerabilities. Auxilium were supplied with a list of IP addresses, in order to enumerate them and test them for potential misconfigurations and security issues.
- Revision of the security configuration of embedded Linux. Based on Linux, the backend system was tested by Auxilium in order to find possible misconfiguration in the system. With experience in embedded systems, IoT devices based on Linux and backend infrastructure testing, common techniques and privilege escalation methodology was conducted targeting the device.

Main Achievements

- Auxilium Cyber Security discovered several critical and high severity vulnerabilities on RETIA's device web portal. Alongside these vulnerabilities there was one OS command injection that gave direct access to the backend system.

- RETIA makes use of several opensource technologies in the device tested by Auxilium. During our testing an undisclosed zero-day vulnerability was found that allows malicious users to create arbitrary files to any system directory, due to improper input validation.
    - Auxilium responsibly disclosed this finding to the developers of the software and helped the open source community to successfully fix the issue.
- Auxilium Cyber Security discovered several high and medium severity vulnerabilities in the underlying system, which could lead to privilege escalation.
- Auxilium Cyber Security trained RETIA's employees regarding the procedures followed in the penetration test and introduced them to the tools used by the team. The aim of the workshop was to train the employees to a level that can perform similar small scale penetration tests autonomously, targeting the tested device.

About RETIA

RETIA is a Czech company founded in 1993, performing its own research and high quality manufacturing in the field of military electronics and recording systems. They have successfully implemented a large number of projects not only for major domestic clients but also for customers in more than 40 countries throughout the world.