Industrial Cellular Router Penetration Test

Advantech Czech

Task

Auxilium Cyber Security was approached by Advantech Czech to conduct a penetration test to determine the exposure of Advantech's industrial cellular router device to targeted attacks by malicious users. Advantech is a global leader in IoT intelligent systems and embedded platforms, developing different types of customized hardware. Considering the importance of security in the industrial sector, one of the critical requirements was to ensure the tested device met the implied level of cyber security.

Solution

Based on our prior experience with hardware penetration testing, we offered to provide thorough security testing of the device. Due to the open and customizable nature of Advantech industrial cellular routers, testing had to be adapted and specialized for its design. Testing of the device was conducted in a manner that simulated malicious user scenarios and attacks which targeted the infrastructure and web portal part of the device, with the phases of the testing being the following:

- **Identify security risks and vulnerabilities on the administration web portal.** The first part of testing was targeting the web portal provided by the device using several custom technologies. The tests conducted to the target web portal comprised automated and manual testing based on industry standards and common web security issues (OWASP Top 10). Additionally, Auxilium was supplied with a list of proposed configurations to apply them to the device and test for possible security issues after applying the proposed secure configuration by the user.
- **Identify security risks and vulnerabilities in the device infrastructure.** Auxilium were supplied with a superuser access to the device, to enumerate the backend system and test for potential misconfigurations and security issues. Additionally, Wi-Fi and SMS testing were conducted to find possible misconfigurations in other entry points of the device, like the command execution with SMS functionality of the device.
- **Review the Security Guidelines.** Due to the open nature of the device, users have complete access with a lot of customizability. To help users configure their device securely, Advantech created a set of recommendations, which Auxilium reviewed and proposed changes that could potentially create security issues for users or might help attackers achieve a better outcome.

The tests were conducted in October 2020 based on the firmware v6.2.6.

Auxilium Cyber Security, s.r.o. · Přístavní 1363/1, Holešovice · CZ-17000 Prague

www.auxiliumcybersec.cz · info@auxiliumcybersec.cz · +420 739 467 470 · +49(0)173 - 704 86 49 | Managing Director: Martin Pozděna · Markus Ganzmann

Registered with the Municipal Court in Prague, Section C, Insert 311555 · Registration number: 08013381 · VAT ID: CZ08013381

Bank account details: Fio banka, a.s. · CZK: 2501605058/2010 · EUR IBAN: CZ63 2010 0000 0023 0160 5061 · USD IBAN: CZ23 2010 0000 0023 0179 2506

Main Achievements

- Auxilium Cyber Security described multiple security deficiencies in the implementation or configuration of device services. The report included possible attack vectors and suggestions how these should be remediated. Auxilium also suggested additional modifications to the device configuration to further reduce the attack surface. A teleconference with the Advantech team was held to pass on this this information and ensure it was well understood.
- Auxilium Cyber Security discovered several omissions and ambiguities in the Security Guidelines that could cause a less secure device configuration. After careful analysis and communication with the client, several improvements have been suggested that lead to a more detailed, security focused and complete document.

About Advantech

Advantech is a global leader in the fields of IoT intelligent systems and embedded platforms. To embrace the trends of IoT, big data, and artificial intelligence, Advantech promotes IoT hardware and software solutions with the Edge Intelligence WISE-PaaS core to assist business partners and clients in connecting their industrial chains. Advantech is also working with business partners to co-create business ecosystems that accelerate the goal of industrial intelligence.