Penetrační test průmyslového mobilního routeru

Advantech Czech

Zadání

Auxilium Cyber Security byla oslovena společností Advantech, aby provedla penetrační test s cílem posoudit kybernetické zabezpečení průmyslového mobilního routeru společnosti Advantech. Firma Advantech je světovým lídrem v oblasti inteligentních systémů IoT a vestavěných systémů a vyvíjí na zakázku různé typy hardwaru. Vzhledem k důležitosti bezpečnosti v průmyslovém sektoru bylo jedním z kritických požadavků zajistit, aby testované zařízení splňovalo předpokládanou úroveň kybernetického zabezpečení.

Postup řešení

Na základě našich předchozích zkušeností s penetračním testováním hardwaru jsme provedli důkladné otestování zabezpečení zařízení. Vzhledem k modifikovatelné povaze průmyslových mobilních routerů Advantech, muselo být i testování přizpůsobeno danému zařízení. Testování zařízení bylo provedeno způsobem, který simuloval škodlivé uživatelské scénáře a útoky, které byly zacíleny na část infrastruktury a portálu webové administrace zařízení, přičemž fáze testování byly následující:

- **Identifikovat bezpečnostní rizika a zranitelná místa na administrativním webovém rozhraní.** Testy zahrnovaly automatizované a manuální testování založené na průmyslových standardech a běžných zranitelnostech ve webových službách (OWASP Top 10). Navíc Auxilium dostalo seznam doporučovaných konfigurací zařízení k otestování možných bezpečnostních problémů po použití navrhované konfigurace uživatelem.
- **Identifikovat bezpečnostní rizika a zranitelná místa v infrastruktuře zařízení.** Auxilium dostalo přístup superuživatele k zařízení, aby mohlo otestovat potenciální nesprávné konfigurace a bezpečnostní problémy. Kromě toho byly provedeny testy Wi-Fi a SMS, aby se zjistily možné nesprávné konfigurace v různých vstupních bodech zařízení, jako je zasílání příkazů pomocí SMS.
- **Posoudit bezpečnostní doporučení (Security Guidelines).** Vzhledem k modifikovatelné povaze zařízení mají uživatelé plný přístup do administrativního webového rozhraní se spoustou možností k vlastnímu přizpůsobení. Aby uživatelé používali bezpečně nakonfigurované zařízení, Advantech vytvořil sadu doporučení, která Auxilium zkontrolovalo a navrhlo změny u bodů, které by potenciálně mohly vytvářet bezpečnostní problémy pro uživatele nebo by mohly vést ke zneužití útočníkem.

Testy byly provedeny v říjnu 2020 na základě firmwaru 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

Hlavní výstupy

- Naši testeři objevili několik bezpečnostních nedostatků při implementaci nebo konfiguraci služeb zařízení. Závěrečná zpráva z bezpečnostního auditu obsahovala možné zranitelnosti a vektory útoku společně s návrhy, jak by měly být odstraněny. Auxilium také navrhlo další úpravy konfigurace zařízení k dalšímu snížení hrozby úspěšného útoku. Kromě písemné závěrečné zprávy proběhl i video hovor, abychom zajistili, že veškeré poznatky budou srozumitelně předány.
- Dále naši testeři objevili několik opomenutí a nejasností v bezpečnostních pokynech, které by mohly způsobit méně bezpečnou konfiguraci zařízení. Po pečlivé analýze a na základě komunikace s klientem bylo navrženo několik vylepšení, která vedou k podrobnějšímu a komplexnějšímu dokumentu zaměřenému na lepší zabezpečení.

O Advantech

Advantech je světovým lídrem v oblasti inteligentních systémů IoT a vestavných platforem. Advantech poskytuje hardwarová a softwarová řešení IoT s jádrem Edge Intelligence WISE-PaaS, která pomáhají obchodním partnerům a klientům při propojování jejich průmyslových řetězců, adopci IoT, big data a umělé inteligence. Advantech také spolupracuje s obchodními partnery na společném vytváření obchodních ekosystémů, které urychlují cíl průmyslové automatizace.