Penetrační test zařízení pro vojenské účely

Retia, a.s.

Úkol

Společnost Auxilium Cyber Security byla oslovena firmou RETIA, aby provedla penetrační test, jehož cílem je zjištění míry rizika cílených útoků na jejich zařízení.

RETIA je česká společnost provádějící vlastní výzkum a výrobu vysoce kvalitní elektroniky pro vojenské účely a záznamových systémů s dodávkami po celém světě. Vzhledem k důležitosti bezpečnosti vojenského vybavení bylo jedním z kritických požadavků zajistit, aby testované zařízení splňovalo dostatečnou úroveň kybernetické bezpečnosti.

Dodané zařízení bylo v době testování stále ve stádiu vývoje SW vybavení. Cílem testování tudíž také bylo využití výstupů testování ke konečné finalizaci SW vybavení testovaného produktu a ke zvýšení jeho odolnosti a bezpečného použití.

Řešení

Na základě našich předchozích zkušeností s hardware a penetračním testováním v oblasti automobilového průmyslu jsme nabídli provedení důkladného testování bezpečnosti zařízení. Vzhledem ke složité a specifické povaze tohoto zařízení muselo být testování přizpůsobeno a specializováno pro tyto potřeby. Testování zařízení probíhalo způsobem, který simuloval scénáře útoků se zaměřením na infrastrukturu a webové rozhraní zařízení, přičemž fáze testování byly následující:

- Identifikovat bezpečnostní rizika a zranitelnosti na webovém portálu pro správu zařízení. První část testování byla zaměřena na webový portál zařízení RETIA, který byl implementován pomocí několika různých veřejně dostupných technologií. Testy provedené na cílovém webovém portálu byly rozděleny na automatizované a ruční testování podle průmyslových standardů a se zaměřením na nejčastější problémy s webovou bezpečností (OWASP Top 10).
- Identifikovat bezpečnostní rizika a zranitelnosti. Auxilium obdrželo seznam IP adres zařízení, které byly prověřeny a otestovány na možné nesprávné konfigurace a problémy se zabezpečením.
- Revize konfigurace zabezpečení vestavěného systému Linux. Linuxový backend byl testován společností Auxilium s cílem detekce možných nesprávných konfigurací systému. Řada testovacích technik a metodologie eskalace oprávnění byly použity díky bohatým zkušenostem s vestavnými systémy, zařízeními IoT založených na Linuxu a backend infrastruktury.

Dosažené cíle

- Auxilium Cyber Security objevila na webovém portálu zařízení RETIA několik kritických a závažných zranitelností. Vedle těchto zranitelností byla objevena možnost injektovat a spouštět příkazy OS, díky čemuž byl umožněn přímý přístup do backend systému.

- RETIA využívá v zařízení testovaném společností Auxilium několik open source technologií. Během našeho testování byla zjištěna nezveřejněná "zero-day" chyba v open source knihovně, která útočníkům umožňuje vytvářet libovolné soubory v libovolném systémovém adresáři v důsledku nesprávně ošetřeného uživatelského vstupu.
    - Společnost Auxilium předala informace o tomto zjištění vývojářům softwaru v rámci tzv. "responsible disclosure" a pomohla open source komunitě úspěšně vyřešit tento problém.
- Auxilium Cyber Security objevila v systému několik zranitelných míst s vysokou a střední závažností, které mohou vést k eskalaci oprávnění.
- Auxilium Cyber Security provedlo školení zaměstnanců společnosti RETIA o postupech používaných při penetračním testu a zasvětila je do používaných nástrojů. Cílem workshopu bylo vyškolit zaměstnance na úroveň, díky které mohou sami v menším rozsahu provádět podobné testy v rámci QA testování.

O společnosti RETIA

RETIA je česká společnost založená v roce 1993, provádějící vlastní výzkum a kvalitní výrobu v oblasti vojenské elektroniky a záznamových systémů. Úspěšně realizovali velké množství projektů nejen pro významné domácí klienty, ale také pro zákazníky ve více než 40 zemích po celém světě.