Jean Pereira

Biztonsági kutatás · Offenzív biztonság · Full-stack fejlesztés

Összetett rendszerek sérülékenységeit kutatom, és biztonsági szoftvereket, valamint saját termékeket fejlesztek böngészőbiztonság, beágyazott és ipari rendszerek, automatizálás és AI területén.

Jean Pascal José Pereira · Németország · LinkedIn · pereira.cv/contact

Profil

Ott találok biztonsági réseket, ahol mások abbahagyják a keresést, és biztonságos szoftvereket fejlesztek összetett problémák megoldására.

Munkám a **Siemens**, **Apple**, **Google**, **Microsoft** és **Nokia** termékeinek és technológiáinak sérülékenységeit, valamint különféle orvostechnikai projekteket is magában foglalja. Jelenleg a biztonsági kutatásra és a szoftvermérnöki munkára összpontosítok.

Emellett a **Veloce** szerzője is vagyok. A kapcsolatfelvételi űrlapon vagy közvetlenül a LinkedIn felületén érhetsz el.

Kiemelt pontok

Négy zero-day a Siemensnél: riasztórendszerek és tűzérzékelők távolról átvéve

Távolról teljesen átvettem a Siemens riasztórendszereinek és tűzérzékelőinek irányítását. Exploitom root hozzáférést, a legmagasabb rendszerjogosultságokat biztosította, bejelentkezési adatok, kattintás vagy az áldozat bármilyen közreműködése nélkül.

Négy ismeretlen sérülékenységet összekapcsoló exploitláncot fejlesztettem, és a teljes átvételt gyakorlatban is bemutattam. Biztonságkritikus riasztástechnika irányításáról volt szó.

A Siemens megerősítette a négy felfedezést: CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Az exploit értékelése CVSS 10.0, a lehető legsúlyosabb besorolás.

Zero-day sérülékenységek kórházakban: vércsoportok módosítva, EKG-riasztások és szellőztetőberendezések kikapcsolva

Egy biztonsági vizsgálatban tizenkét gyártó eszközeiben 22 korábban ismeretlen sérülékenységet fedeztem fel, és működő exploitokkal bemutattam az EKG-riasztások kikapcsolását, steril műtők szellőzésének leállítását, valamint vércsoportok és allergiaadatok módosítását. Saját SOP/CORS-megkerüléseimmel távoli támadásokat is bemutattam az internetről közvetlenül el nem érhető belső eszközök ellen.

A vizsgált gyártók között van a ZEISS, MOXA, Zebra, Dedalus Labor és Tetronik. A Golem 2024-es riportja szerint az eszközöket több ezer további kórházban és egészségügyi intézményben használták. Koordináltam a bejelentést és támogattam a javításokat. Újságírók követték a teljes folyamatot, a gyártók értesítésétől a javításokhoz nyújtott támogatásomig.

Sérülékenységek több mint 40 hatóságnál, az OBI-nál, a REWE-nél és a Fraunhofer Intézetnél

45 önkormányzatnál és vállalatnál tártam fel sérülékenységeket, és jelentettem azokat a felelősöknek. Az OBI webes hibája felhasználói munkamenetek átvételét és a belső tartalomkezelő adataihoz való hozzáférést tette lehetővé.

Sok önkormányzat kijavította a hibákat. Az OBI a nyilvános vita után leállította az érintett oldalt. A Golem és a WirtschaftsWoche dokumentálta a kutatást és a vállalatok reakcióit.

Tapasztalat

2023. jún. - jelenleg

CEO · CTO · CYTRES GmbH
A vállalat alapítása és vezetése, szoftverfejlesztési és kiberbiztonsági kutatási fókuszszal.

2016. dec. - 2019. aug.

Kiberbiztonsági tutor · CIC (Cambridge Innovation Center) · Rotterdam, Hollandia
Kiberbiztonsági workshopokat és műszaki képzéseket tartottam.

2016. dec. - 2019. aug.

Senior biztonsági tanácsadó · Base Cyber Security · Rotterdam, Hollandia
Vezettem a műszaki csapatot, valamint betanítottam és képeztem az új munkatársakat az elvárt műszaki szintig.

2019

Alapító · CEO · CTO · Secbiz IT Security GmbH

- Kiberbiztonsági vállalat alapítója és műszaki vezetője.
- Ipari/OT- és alkalmazásbiztonsági kutatás és tanácsadás.
- Élő SCADA-demonstráció a Hannover Messe 2019 rendezvényen.

Veloce

A Veloce a saját JavaScript/TypeScript runtime-om agentic codinghoz: olyan célplatform, amelyen a kódoló ügynökök teljes, olvasható, auditálható és azonnal futtatható alkalmazásokat hozhatnak létre anélkül, hogy előbb npm-függőségeket, frameworköket, build eszközöket és deployment-ragasztást kellene összerakniuk.

A runtime eleve tartalmazza a fontos építőelemeket: korlátozó sandbox- és jogosultságmodellt, HTTP-szervert, SQLite-ot és PostgreSQL-t ORM-mel és KV-tárral, böngésző- és desktopfunkciókat, valamint önálló natív binárisba történő csomagolást. A számításigényes útvonalak JavaScript/TypeScriptből Rust-alapú natív kernelekre vagy WebAssemblyre szervezhetők ki. A cél olyan szoftver, amelyet az ügynökök megbízhatóan generálhatnak, az emberek továbbra is megértenek, a rendszerek pedig a lehető legkevesebb mozgó alkatrésszel futtathatnak.

Szakértelem

Beágyazott rendszerek, OT és orvostechnika

Sérülékenységkutatás firmware-ben és hálózatba kapcsolt eszközökben: tűzjelző rendszerek, ipari vezérlők (SCADA), kórházi és orvostechnikai eszközök.

Exploitfejlesztés

Egyetlen memory corruption hibától a teljes exploit láncig távoli root hozzáféréssel.

Böngésző- és webbiztonság

SOP/CORS megkerülések, támadási útvonalak belső hálózati eszközökhöz, XSS és alkalmazásbiztonság.

Felelős közzététel

Bejelentés és koordináció gyártókkal és üzemeltetőkkel, nagyvállalatoktól önkormányzatokig, beleértve a javítás támogatását.

Saját eszközök

Eszközök és automatizálás sérülékenységkereséshez és penetrációs teszteléshez, AI-támogatott workflow-kkal is. A Veloce JavaScript/TypeScript runtime szerzője.

Kutatás

Év	Kutatás / sérülékenység	Forrás
2024	Siemens ProductCERT, SSA-333468 - CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904; Remote Code Execution (root)	Siemens
2024	Siemens InterMesh - CISA ICS Advisory ICSA-24-303-01	CISA-bejegyzés a CIRCL-nél
2013	Apple Motion - CVE-2013-6114 - sérülékenység	Apple
2014	Apple Web Server - biztonsági kutatás, 2014. február	Apple
2012	Nokia Hall of Fame - biztonsági kutatás, 2012. december	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit-modul	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq-archívum
2012	PhpTax - CVE-2012-10037 - Remote Command Injection	OpenCVE
2012	b2ePMS - CVE-2012-6626 - SQL Injection / Authentication Bypass	Bugtraq
2012	HCView - Remote Code Execution - BID 55819	Bugtraq
2012	DomsHttpd - Remote Denial of Service - BID 54478	Bugtraq
2012	CommPort - SQL Injection - BID 55239	Bugtraq
2012	Arctic Torrent - Memory Corruption - BID 55833	Bugtraq

Év	Kutatás / sérülékenység	Forrás
2012	plow .plowrc - Buffer Overflow - BID 54290	Bugtraq
2012	Internet Explorer - XSS Filter Bypass - Exploit-DB 22100	VulDB

Sajtó

Év	Eredeti cikk	Médium
2025	Beszámoló a Securitas / Marvelit felelős sebezhetőség-bejelentéséről	Security-Insider
2022	Rádióműsor a kiberbiztonságról és az etikus hackelésről	WDR
2024	ÖAG szakértői beszélgetés: Biztonság 4.0 - kiberbiztonság és MI-alapú védelem	medianet (Ausztria)
2024	Biztonsági sérülékenységek kórházakban: veszélyben a betegek	Golem
2024	Böngésző SOP/CORS és belső hálózati eszközök	CYTRES Research
2024	Jean Pereira nyilvános biztonsági bejelentése dokumentált javítási frissítéssel	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Szakértői beszélgetés Tursky államtitkárral a digitalizációról, az MI-ről és a kiberbiztonságról	KURIER (Ausztria)
2023	Részvétel kiberbiztonsági szakértőként az ÖAG Super Tuesday rendezvényen	LEADERSNET (Ausztria)
2022	Podcast #51: Ethical Hacker - biztonsági kutatás és szakmai pálya	IDG TechTalk / COMPUTERWOCHE
2022	IT-biztonsági sérülékenység Köln városánál	Kölner Stadt-Anzeiger
2022	Az adatvédelmi biztos vizsgálatot indít egy figyelmen kívül hagyott, bejelentett biztonsági rés miatt	WirtschaftsWoche
2022	Felelős sebezhetőség-bejelentés / 45 szervezet	Golem
2022	Beszámoló az OBI-ról és hatóságokról	connect professional
2020	Keynote a böngésző- és alkalmazásbiztonságról	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: élő SCADA/ICS-hackelés	Hannover Messe / MittelstandsWiki
2019	Interjú: "Több hackerre van szükségünk"	atp magazin
2019	Kibertámadások és darknet - interjú Jean Pereirával	Podcast "IT'S IN YOU"
2018	SEO-DAY: a Chrome feltörése és az SSL megkerülése 2018-ban	Host Europe
2018	Biztonsági előadás a SEO-DAY 2018 szuperpaneljében	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker és a SECBIZ alapítója az előadók között	DSS IT SEC / Riga