Jean Pereira

Bezpečnostní výzkum · Ofenzivní bezpečnost · Full-stack vývoj

Zkoumám zranitelnosti složitých systémů a vyvíjím bezpečnostní software i vlastní produkty v oblasti zabezpečení prohlížečů, embedded a průmyslových systémů, automatizace a AI.

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

Profil

Nacházím bezpečnostní chyby tam, kde ostatní přestávají hledat, a vyvíjím bezpečný software, který řeší složité problémy.

Moje práce zahrnuje zranitelnosti v produktech a technologiích **Siemens**, **Apple**, **Google**, **Microsoft** a **Nokia** i různé projekty v oblasti zdravotnické techniky. V současnosti se zaměřuji na bezpečnostní výzkum a softwarové inženýrství.

Jsem také autorem **Veloce**. Můžeš mě kontaktovat prostřednictvím kontaktního formuláře nebo přímo na LinkedIn.

Hlavní body

Čtyři zero-day u Siemens: alarmy a požární hlásiče převzaty na dálku

Na dálku jsem plně převzal alarmy a požární hlásiče Siemens. Můj exploit mi poskytl přístup root, nejvyšší systémová oprávnění, bez přihlašovacích údajů, kliknutí či jiné součinnosti oběti.

Vyvinul jsem řetězec exploitů spojující čtyři neznámé zranitelnosti a úplné převzetí prakticky prokázal. Šlo o kontrolu nad poplachovou technikou zásadní pro bezpečnost.

Siemens potvrdil čtyři nálezy jako CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Exploit získal hodnocení CVSS 10.0, maximální možná závažnost.

Zero-day v nemocnicích: krevní skupiny změněny, alarmy EKG a větrací zařízení vypnuty

Při bezpečnostní analýze jsem objevil 22 dosud neznámých zranitelností v zařízeních dvanácti výrobců a útoky prokázal funkčními exploity: vypnutí alarmů EKG, přerušení ventilace sterilních operačních sálů a manipulaci s krevními skupinami a alergiemi. Vyvinul jsem také obcházení SOP/CORS a demonstroval vzdálené útoky na interní zařízení nepřístupná přímo z internetu.

Mezi zkoumané výrobce patří ZEISS, MOXA, Zebra, Dedalus Labor a Tetronik. Podle reportáže Golem z roku 2024 byla dotčená zařízení nasazena v tisících dalších nemocnic a zdravotnických zařízení. Koordinoval jsem oznámení a podpořil nápravu. Novináři sledovali celý proces, od oznámení výrobcům až po mou podporu při odstraňování zranitelností.

Zranitelnosti ve více než 40 úřadech, OBI, REWE a Fraunhoferově institutu

Odhalil jsem zranitelnosti ve 45 městských úřadech a firmách a oznámil je odpovědným týmům. U OBI webová zranitelnost umožňovala převzetí uživatelských relací a čtení informací z interního redakčního systému.

Mnohé úřady chyby opravily. OBI po veřejném sporu postižený web odstavilo. Golem a WirtschaftsWoche zdokumentovaly výzkum a reakce firem.

Zkušenosti

červen 2023 - současnost

CEO · CTO · CYTRES GmbH
Založil a vedl jsem společnost se zaměřením na vývoj softwaru a výzkum kybernetické bezpečnosti.

prosinec 2016 - srpen 2019

Tutor kybernetické bezpečnosti · CIC (Cambridge Innovation Center) · Rotterdam, Nizozemsko
Vedl jsem workshopy kybernetické bezpečnosti a technická školení.

prosinec 2016 - srpen 2019

Seniorní bezpečnostní poradce · Base Cyber Security · Rotterdam, Nizozemsko
Vedl jsem technický tým a zaučoval a školil nové zaměstnance na požadovanou technickou úroveň.

2019

Zakladatel · CEO · CTO · Secbiz IT Security GmbH

- Zakladatel a technický vedoucí bezpečnostní firmy.

- Výzkum a poradenství pro průmyslovou/OT a aplikační bezpečnost.
- Živá ukázka útoku na SCADA na Hannover Messe 2019.

Veloce

Veloce je můj JavaScript/TypeScript runtime pro agentic coding: cílová platforma, na které mohou programovací agenti vytvářet kompletní aplikace, které jsou čitelné, auditovatelné a rovnou spustitelné, bez skládání npm závislostí, frameworků, build nástrojů a deploymentové režie.

Runtime obsahuje klíčové stavební bloky přímo: restriktivní sandbox a model oprávnění, HTTP server, SQLite a PostgreSQL s ORM a KV úložištěm, funkce pro browser a desktop a balení do samostatného nativního binárního souboru. Výpočetně náročné části lze z JavaScriptu/TypeScriptu přesunout do nativních kernelů založených na Rustu nebo do WebAssembly. Cílem je software, který mohou agenti spolehlivě generovat, lidé mu stále rozumějí a systémy ho provozují s minimem pohyblivých částí.

Odbornost

Embedded, OT a zdravotnická technika

Výzkum zranitelností ve firmwaru a připojených zařízeních: požární signalizace, průmyslové řídicí systémy (SCADA), nemocniční a zdravotnická zařízení.

Vývoj exploitů

Od jednotlivé chyby memory corruption až po úplný exploit chain se vzdáleným root přístupem.

Bezpečnost prohlížečů a webu

SOP/CORS bypassy, útočné cesty k zařízením ve vnitřních sítích, XSS a bezpečnost aplikací.

Odpovědné zveřejnění

Oznamování a koordinace s výrobci a provozovateli, od velkých společností po městské úřady, včetně podpory při nápravě.

Vlastní nástroje

Nástroje a automatizace pro hledání zranitelností a penetrační testování, včetně workflow s podporou AI. Autor JavaScript/TypeScript runtime Veloce.

Výzkum

Rok	Výzkum / zranitelnost	Zdroj
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	záznam CISA u CIRCL
2013	Apple Motion - CVE-2013-6114 - zranitelnost	Apple
2014	Apple Web Server - bezpečnostní výzkum, únor 2014	Apple
2012	Nokia Hall of Fame - bezpečnostní výzkum, prosinec 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - modul Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	archiv Bugtraq
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
2012	plow .plowrc - Buffer Overflow - BID 54290	Bugtraq
2012	Internet Explorer - XSS Filter Bypass - Exploit-DB 22100	VulDB

Média

Rok	Původní článek	Médium
2025	Zpravodajství o responsible disclosure u Securitas / Marvelit	Security-Insider
2022	Rozhlasový příspěvek o kybernetické bezpečnosti a etickém hackingu	WDR
2024	Expertní diskuse ÖAG: Bezpečnost 4.0 - kybernetická bezpečnost a obrana pomocí AI	medianet (Rakousko)
2024	Bezpečnostní zranitelnosti v nemocnicích: pacienti v ohrožení	Golem
2024	Browser SOP/CORS a zařízení ve vnitřní síti	CYTRES Research
2024	Veřejné bezpečnostní oznámení Jeana Pereiry s doloženou aktualizací nápravy	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Expertní diskuse se státním tajemníkem Turskym o digitalizaci, AI a kybernetické bezpečnosti	KURIER (Rakousko)
2023	Účast jako expert na kybernetickou bezpečnost na ÖAG Super Tuesday	LEADERSNET (Rakousko)
2022	Podcast #51: Ethical Hacker - bezpečnostní výzkum a profesní cesta	IDG TechTalk / COMPUTERWOCHE
2022	Bezpečnostní zranitelnost IT u města Kolín nad Rýnem	Kölner Stadt-Anzeiger
2022	Pověřenkyně pro ochranu osobních údajů vyšetřuje ignorovanou nahlášenou bezpečnostní chybu	WirtschaftsWoche
2022	Responsible disclosure / 45 organizací	Golem
2022	Zpráva o OBI a veřejných institucích	connect professional
2020	Keynote o bezpečnosti prohlížečů a aplikací	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: živé hackování SCADA/ICS	Hannover Messe / MittelstandsWiki
2019	Rozhovor "Potřebujeme více hackerů"	atp magazin
2019	Kybernetické útoky a darknet - rozhovor s Jeanem Pereirou	Podcast "IT'S IN YOU"
2018	SEO-DAY: jak hacknout Chrome a obejít SSL v roce 2018	Host Europe
2018	Bezpečnostní přednáška v superpanelu SEO-DAY 2018	SEO-DAY / Online--Profession
2018	International Cyber Security Conference: Ethical Hacker a zakladatel SECBIZ mezi řečníky	DSS IT SEC / Riga