Jean Pereira

Bezpečnostný výskum · Ofenzívna bezpečnosť · Full-stack vývoj

Skúmam zraniteľnosti komplexných systémov a vyvíjam bezpečnostný softvér aj vlastné produkty v oblasti bezpečnosti prehliadačov, embedded a priemyselných systémov, automatizácie a AI.

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

Profil

Nachádzam bezpečnostné chyby tam, kde ostatní prestávajú hľadať, a vyvíjam bezpečný softvér, ktorý rieši zložité problémy.

Moja práca zahŕňa zraniteľnosti v produktoch a technológiách **Siemens**, **Apple**, **Google**, **Microsoft** a **Nokia** aj rôzne projekty v oblasti zdravotníckej techniky. V súčasnosti sa zameriavam na bezpečnostný výskum a softvérové inžinierstvo.

Som tiež autorom **Veloce**. Môžeš ma kontaktovať prostredníctvom kontaktného formulára alebo priamo na LinkedIn.

Hlavné body

Štyri zero-day v Siemens: alarmy a požiarne hlásiče prevzaté na diaľku

Na diaľku som úplne prevzal alarmy a požiarne hlásiče Siemens. Môj exploit mi poskytol prístup root, najvyššie systémové oprávnenia, bez prihlasovacích údajov, kliknutia či inej súčinnosti obete.

Vyvinul som reťazec exploitov spájajúci štyri neznáme zraniteľnosti a úplné prevzatie prakticky preukázal. Išlo o kontrolu nad poplachovou technikou zásadnou pre bezpečnosť.

Siemens potvrdil štyri nálezy ako CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Exploit získal hodnotenie CVSS 10.0, maximálna možná závažnosť.

Zero-day v nemocniciach: krvné skupiny zmenené, alarmy EKG a vetracie zariadenia vypnuté

Pri bezpečnostnej analýze som objavil 22 dovtedy neznámych zraniteľností v zariadeniach dvanástich výrobcov a útoky preukázal funkčnými exploitmi: vypnutie alarmov EKG, prerušenie ventilácie sterilných operačných sál a manipuláciu s krvnými skupinami a alergiami. Vyvinul som tiež obchádzanie SOP/CORS a demonštroval vzdialené útoky na interné zariadenia neprístupné priamo z internetu.

Medzi skúmaných výrobcov patria ZEISS, MOXA, Zebra, Dedalus Labor a Tetronik. Podľa reportáže Golem z roku 2024 boli zariadenia nasadené v tisícoch ďalších nemocníc a zdravotníckych zariadení. Koordinoval som oznámenia a podporil nápravu. Novinári sledovali celý proces, od oznámenia výrobcom až po moju podporu pri odstraňovaní zraniteľností.

Zraniteľnosti vo viac ako 40 úradoch, OBI, REWE a Fraunhoferovom inštitúte

Odhalil som zraniteľnosti v 45 mestských úradoch a firmách a oznámil ich zodpovedným tímom. V OBI webová zraniteľnosť umožňovala prevzatie používateľských relácií a čítanie informácií z interného redakčného systému.

Mnohé úrady chyby opravili. OBI po verejnom spore dotknutý web odstavilo. Golem a WirtschaftsWoche zdokumentovali výskum a reakcie firiem.

Skúsenosti

6/2023 - súčasnosť

CEO · CTO · CYTRES GmbH
Založil a viedol som spoločnosť so zameraním na vývoj softvéru a výskum kybernetickej bezpečnosti.

12/2016 - 8/2019

Tutor kybernetickej bezpečnosti · CIC (Cambridge Innovation Center) · Rotterdam, Holandsko
Viedol som workshopy kybernetickej bezpečnosti a technické školenia.

12/2016 - 8/2019

Senior bezpečnostný poradca · Base Cyber Security · Rotterdam, Holandsko
Viedol som technický tím a zaškoľoval a školil nových zamestnancov na požadovanú technickú úroveň.

2019

Zakladateľ · CEO · CTO · Secbiz IT Security GmbH

- Zakladateľ a technický vedúci bezpečnostnej spoločnosti.
- Výskum a poradenstvo v oblasti priemyselnej/OT a aplikačnej bezpečnosti.
- Živá ukážka útoku na SCADA na Hannover Messe 2019.

Veloce

Veloce je môj JavaScript/TypeScript runtime pre agentic coding: cieľová platforma, na ktorej môžu programovacie agenty vytvárať kompletné aplikácie, ktoré sú čitateľné, auditovateľné a priamo spustiteľné, bez skladania npm závislostí, frameworkov, build nástrojov a deploymentovej réžie.

Runtime obsahuje kľúčové stavebné bloky priamo: reštriktívny sandbox a model oprávnení, HTTP server, SQLite a PostgreSQL s ORM a KV úložiskom, browserové a desktopové funkcie a balenie do samostatného natívneho binárneho súboru. Výpočtovo náročné časti možno z JavaScriptu/TypeScriptu presunúť do natívnych kernelov založených na Ruste alebo do WebAssembly. Cieľom je softvér, ktorý môžu agenty spoľahlivo generovať, ľudia mu stále rozumejú a systémy ho spúšťajú s minimom pohyblivých častí.

Odbornosť

Embedded, OT a zdravotnícka technika

Výskum zraniteľností vo firmvéri a pripojených zariadeniach: požiarna signalizácia, priemyselné riadiace systémy (SCADA), nemocničné a zdravotnícke zariadenia.

Vývoj exploitov

Od jednej chyby memory corruption až po úplný exploit chain so vzdialeným root prístupom.

Bezpečnosť prehliadačov a webu

SOP/CORS bypassy, útočné cesty k zariadeniam vo vnútorných sieťach, XSS a bezpečnosť aplikácií.

Zodpovedné zverejnenie

Oznamovanie a koordinácia s výrobcami a prevádzkovateľmi, od veľkých spoločností po mestské úrady, vrátane podpory pri náprave.

Vlastné nástroje

Nástroje a automatizácia na hľadanie zraniteľností a penetračné testovanie, vrátane workflow s podporou AI. Autor JavaScript/TypeScript runtime Veloce.

Výskum

Rok	Výskum / zraniteľnosť	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 v CIRCL
2013	Apple Motion - CVE-2013-6114 - zraniteľnosť	Apple
2014	Apple Web Server - bezpečnostný výskum, február 2014	Apple
2012	Nokia Hall of Fame - bezpečnostný výskum, december 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - modul Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	archív 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

Rok	Výskum / zraniteľnosť	Zdroj
2012	plow .plowrc - Buffer Overflow - BID 54290	Bugtraq
2012	Internet Explorer - XSS Filter Bypass - Exploit-DB 22100	VulDB

Médiá

Rok	Pôvodný článok	Médium
2025	Spravodajstvo o responsible disclosure v Securitas / Marvelit	Security-Insider
2022	Rozhlasový príspevok o kybernetickej bezpečnosti a etickom hackingu	WDR
2024	Expertná diskusia ÖAG: Bezpečnosť 4.0 - kybernetická bezpečnosť a obrana pomocou AI	medianet (Rakúsko)
2024	Bezpečnostné zraniteľnosti v nemocniciach: pacienti v ohrození	Golem
2024	Browser SOP/CORS a zariadenia vo vnútornej sieti	CYTRES Research
2024	Verejné bezpečnostné oznámenie Jeana Pereiru s doloženou aktualizáciou nápravy	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Expertná diskusia so štátnym tajomníkom Turskym o digitalizácii, AI a kybernetickej bezpečnosti	KURIER (Rakúsko)
2023	Účasť ako expert na kybernetickú bezpečnosť na ÖAG Super Tuesday	LEADERSNET (Rakúsko)
2022	Podcast #51: Ethical Hacker - bezpečnostný výskum a profesijná cesta	IDG TechTalk / COMPUTERWOCHE
2022	Bezpečnostná zraniteľnosť IT v meste Kolín nad Rýnom	Kölner Stadt-Anzeiger
2022	Poverenkyňa pre ochranu osobných údajov vyšetruje ignorovanú nahlásenú bezpečnostnú chybu	WirtschaftsWoche
2022	Responsible disclosure / 45 organizácií	Golem
2022	Správa o OBI a verejných inštitúciách	connect professional
2020	Keynote o bezpečnosti prehliadačov a aplikácií	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: živé hackovanie SCADA/ICS	Hannover Messe / MittelstandsWiki
2019	Rozhovor "Potrebujeme viac hackerov"	atp magazin
2019	Kybernetické útoky a darknet - rozhovor s Jeanom Pereirom	Podcast "IT'S IN YOU"
2018	SEO-DAY: ako hacknúť Chrome a obísť SSL v roku 2018	Host Europe
2018	Bezpečnostná prednáška v superpaneli SEO-DAY 2018	SEO-DAY / Online--Profession
2018	International Cyber Security Conference: Ethical Hacker a zakladateľ SECBIZ medzi rečníkmi	DSS IT SEC / Riga