Jean Pereira

Sikkerhedsforskning · Offensiv sikkerhed · Fullstackudvikling

Jeg undersøger sårbarheder i komplekse systemer og udvikler sikkerhedssoftware og egne produkter inden for browsersikkerhed, embedded og industrielle systemer, automatisering og AI.

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

Profil

Jeg finder sikkerhedshuller dér, hvor andre holder op med at lede, og bygger sikker software, der løser komplekse problemer.

Mit arbejde omfatter sårbarheder i produkter og teknologier fra **Siemens**, **Apple**, **Google**, **Microsoft** og **Nokia** samt forskellige projekter inden for medicoteknik. Mit fokus er i øjeblikket på sikkerhedsforskning og softwareudvikling.

Jeg er også skaberen af **Veloce**. Du kan kontakte mig via kontaktformularen eller direkte på LinkedIn.

Højdepunkter

Fire zero-days hos Siemens: alarmsystemer og branddetektorer overtaget på afstand

Jeg overtog på afstand den fulde kontrol over alarmsystemer og branddetektorer fra Siemens. Min exploit gav root-adgang, de højeste systemrettigheder, uden loginoplysninger, klik eller anden medvirken fra offeret.

Jeg udviklede en exploitkæde med fire ukendte sårbarheder og demonstrerede den fulde overtagelse i praksis. Det handlede om kontrol over sikkerhedskritisk alarmteknik.

Siemens bekræftede de fire fund som CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Exploiten fik vurderingen CVSS 10.0, den maksimalt mulige alvorlighed.

Zero-days på hospitaler: blodtyper manipuleret, EKG-alarmer og ventilationsanlæg slukket

Under en sikkerhedsanalyse opdagede jeg 22 hidtil ukendte sårbarheder i enheder fra tolv producenter og demonstrerede angrebene med fungerende exploits: deaktivering af EKG-alarmer, afbrydelse af ventilation i sterile operationsstuer og manipulation af blodgrupper og allergioplysninger. Jeg udviklede også SOP/CORS-bypasses til fjernangreb på interne enheder uden direkte internetadgang.

Undersøgte producenter omfatter ZEISS, MOXA, Zebra, Dedalus Labor og Tetronik. Ifølge Golems reportage fra 2024 blev enhederne anvendt på tusindvis af andre hospitaler og medicinske institutioner. Jeg koordinerede rapporteringen og støttede udbedringen. Journalister fulgte hele processen, fra rapportering til producenterne til min støtte til udbedringen.

Sårbarheder hos over 40 myndigheder, OBI, REWE og Fraunhofer-instituttet

Jeg fandt sårbarheder hos 45 kommuner og virksomheder og rapporterede dem til de ansvarlige. Hos OBI muliggjorde en websårbarhed overtagelse af brugersessioner og adgang til oplysninger i det interne indholdssystem.

Mange kommuner rettede fejlene. OBI tog den berørte hjemmeside offline efter den offentlige strid. Golem og WirtschaftsWoche dokumenterede forskningen og virksomhedernes reaktioner.

Erfaring

jun. 2023 - nu

CEO · CTO · CYTRES GmbH
Grundlagde og ledede virksomheden med fokus på softwareudvikling og cybersikkerhedsforskning.

dec. 2016 - aug. 2019

Tutor i cybersikkerhed · CIC (Cambridge Innovation Center) · Rotterdam, Nederlandene
Afholdt workshops i cybersikkerhed og tekniske kurser.

dec. 2016 - aug. 2019

Senior sikkerhedsrådgiver · Base Cyber Security · Rotterdam, Nederlandene
Ledede det tekniske team og oplærte nye medarbejdere til det krævede tekniske niveau.

2019

Grundlægger · CEO · CTO · Secbiz IT Security GmbH

- Grundlægger og teknisk leder af en cybersikkerhedsvirksomhed.

- Forskning og rådgivning om industriel/OT- og applikationssikkerhed.
- Live SCADA-demonstration på Hannover Messe 2019.

Veloce

Veloce er min JavaScript/TypeScript-runtime til agentic coding: en målplatform, hvor kodeagenter kan skabe komplette applikationer, der er læsbare, auditerbare og direkte kørbare uden først at samle npm-afhængigheder, frameworks, build-værktøjer og deployment-glue.

Runtime'en har de vigtige byggesten indbygget: en restriktiv sandbox og rettighedsmodel, HTTP-server, SQLite og PostgreSQL med ORM og KV-lager, browser- og desktopfunktioner samt pakning til en selvstændig native binary. Beregningstunge dele kan flyttes fra JavaScript/TypeScript til Rust-baserede native kernels eller WebAssembly. Målet er software, som agenter kan generere pålideligt, mennesker stadig kan forstå, og systemer kan køre med så få bevægelige dele som muligt.

Ekspertise

Embedded, OT og medicinsk teknologi

Sårbarhedsforskning i firmware og forbundne enheder: brandalarmsystemer, industrielle styringer (SCADA), hospitals- og medicinsk udstyr.

Exploit-udvikling

Fra en enkelt memory-corruption-fejl til en komplet exploit-kæde med fjern root-adgang.

Browser- og websikkerhed

SOP/CORS-bypasses, angrebsveje til enheder på interne netværk, XSS og applikationssikkerhed.

Ansvarlig disclosure

Rapportering og koordinering med producenter og operatører, fra store virksomheder til kommunale myndigheder, inklusive støtte til afhjælpning.

Egne værktøjer

Værktøjer og automatisering til sårbarhedssøgning og penetrationstest, inklusive AI-assisterede workflows. Skaber af JavaScript/TypeScript-runtimen Veloce.

Forskning

År	Forskning / sårbarhed	Kilde
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-post hos CIRCL
2013	Apple Motion - CVE-2013-6114 - sårbarhed	Apple
2014	Apple Web Server - sikkerhedsforskning, februar 2014	Apple
2012	Nokia Hall of Fame - sikkerhedsforskning, december 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit-modul	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq-arkiv
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

Presse

År	Original artikel	Medie
2025	Dækning af responsible disclosure hos Securitas / Marvelit	Security-Insider
2022	Radioindslag om cybersikkerhed og etisk hacking	WDR
2024	ÖAG-ekspertsamtale: Sikkerhed 4.0 - cybersikkerhed og AI-baseret forsvar	medianet (Østrig)
2024	Sikkerhedssårbarheder på hospitaler: patienter i fare	Golem
2024	Browser-SOP/CORS og enheder på det interne netværk	CYTRES Research
2024	Offentlig sikkerhedsmeddelelse fra Jean Pereira med dokumenteret opdatering om udbedringen	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Ekspertsamtale med statssekretær Tursky om digitalisering, AI og cybersikkerhed	KURIER (Østrig)
2023	Deltog som cybersikkerhedsekspert ved ÖAG Super Tuesday	LEADERSNET (Østrig)
2022	Podcast #51: Ethical Hacker - sikkerhedsforskning og karriereforløb	IDG TechTalk / COMPUTERWOCHE
2022	IT-sikkerhedssårbarhed hos byen Köln	Kölner Stadt-Anzeiger
2022	Databeskyttelseskommissæren undersøger en indberettet sikkerhedssårbarhed, som blev ignoreret	WirtschaftsWoche
2022	Responsible disclosure / 45 organisationer	Golem
2022	Beretning om OBI og offentlige myndigheder	connect professional
2020	Keynote om browser- og applikationssikkerhed	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: live SCADA/ICS-hacking	Hannover Messe / MittelstandsWiki
2019	Interview "Vi har brug for flere hackere"	atp magazin
2019	Cyberangreb & darknet - interview med Jean Pereira	Podcast "IT'S IN YOU"
2018	SEO-DAY: sådan hacker man Chrome og omgår SSL i 2018	Host Europe
2018	Sikkerhedsoplæg i superpanelet på SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker og SECBIZ-grundlægger blandt talerne	DSS IT SEC / Riga