Jean Pereira

پژوهش امنیت · امنیت تهاجمی · توسعه Full-Stack

آسیب‌پذیری‌های سامانه‌های پیچیده را بررسی می‌کنم و در حوزه امنیت مرورگر، سامانه‌های تعبیه‌شده و صنعتی، خودکارسازی و هوش مصنوعی، نرم‌افزار امنیتی و محصولات مستقل خودم را توسعه می‌دهم.

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

---

نمایه

آسیب‌پذیری‌های امنیتی را جایی پیدا می‌کنم که دیگران دست از جست‌وجو می‌کشند و نرم‌افزارهای امنی می‌سازم که مسائل پیچیده را حل می‌کنند.

کار من شامل آسیب‌پذیری‌هایی در محصولات و فناوری‌های **Microsoft**، **Google**، **Apple**، **Siemens** و **Nokia** و همچنین پروژه‌های گوناگون در حوزه فناوری پزشکی است. تمرکز فعلی من بر پژوهش امنیت و مهندسی نرم‌افزار است.

همچنین سازنده‌ی **Veloce** هستم. می‌توانی از طریق فرم تماس یا مستقیماً در LinkedIn با من تماس بگیری.

نکات برجسته

چهار آسیب‌پذیری روز صفر در **Siemens**: سامانه‌های هشدار و آشکارسازهای حریق از راه دور در اختیار گرفته شدند

سامانه‌های هشدار و آشکارسازهای حریق Siemens را کاملاً از راه دور در اختیار گرفتم. اکسپلویت من دسترسی root، یعنی بالاترین اختیارات سیستم، را فراهم کرد؛ بدون اطلاعات ورود، کلیک یا هرگونه تعامل قربانی.

زنجیره‌ای از چهار آسیب‌پذیری ناشناخته توسعه دادم و تصاحب کامل را در عمل نشان دادم. موضوع، کنترل فناوری هشدار حیاتی برای ایمنی بود.

Siemens هر چهار یافته را با شناسه‌های CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904 تأیید کرد. اکسپلویت امتیاز CVSS 10.0 را دریافت کرد؛ یعنی حداکثر شدت خطر ممکن.

روز صفر در بیمارستان‌ها: گروه‌های خونی تغییر داده شدند، هشدارهای نوار قلب و دستگاه‌های تهویه خاموش شدند

در یک ارزیابی امنیتی، ۲۲ آسیب‌پذیری ناشناخته در دستگاه‌های دوازده سازنده کشف کردم و حملات را با اکسپلویت‌های عملی نشان دادم: خاموش‌کردن هشدارهای نوار قلب، قطع تهویه اتاق‌های عمل استریل و تغییر گروه خونی و اطلاعات حساسیت. همچنین با توسعه روش‌های دورزدن SOP/CORS، حمله از راه دور به دستگاه‌های داخلی بدون دسترسی مستقیم از اینترنت را نشان دادم.

سازندگان بررسی‌شده شامل ZEISS، MOXA، Zebra، Dedalus Labor و Tetronik هستند. طبق گزارش Golem در سال ۲۰۲۴، دستگاه‌ها در هزاران بیمارستان و مرکز درمانی دیگر استفاده می‌شدند. افشای مسئولانه و پیگیری رفع مشکلات را هماهنگ کردم. روزنامه‌نگاران تمام فرایند را، از اطلاع‌رسانی به سازندگان تا پشتیبانی من در رفع آسیب‌پذیری‌ها، دنبال کردند.

آسیب‌پذیری‌ها در بیش از ۴۰ نهاد دولتی، **REWE**، **OBI** و مؤسسه فراونهوفر

در ۴۵ شهرداری و شرکت آسیب‌پذیری کشف کردم و به مسئولان اطلاع دادم. در OBI، یک آسیب‌پذیری وب امکان تصاحب نشست کاربران و خواندن اطلاعات سامانه داخلی مدیریت محتوا را فراهم می‌کرد.

بسیاری از شهرداری‌ها مشکلات را رفع کردند. OBI پس از مناقشه عمومی سایت مربوط را از دسترس خارج کرد. Golem و WirtschaftsWoche پژوهش و واکنش شرکت‌ها را مستند کردند.

سوابق

خرداد ۱۴۰۲ - اکنون

CEO · CTO · CYTRES GmbH

شرکت را با تمرکز بر توسعه‌ی نرم‌افزار و پژوهش امنیت سایبری تأسیس و مدیریت کردم.

آذر ۱۳۹۵ - مرداد ۱۳۹۸

مدرس امنیت سایبری · CIC (Cambridge Innovation Center) · Rotterdam, هلند

کارگاه‌های امنیت سایبری و دوره‌های آموزشی فنی برگزار کردم.

آذر ۱۳۹۵ - مرداد ۱۳۹۸

مشاور ارشد امنیت · Base Cyber Security · Rotterdam, هلند

تیم فنی را هدایت کردم و کارکنان جدید را تا سطح فنی موردنیاز آموزش دادم.

2019

بنیان‌گذار · CEO · CTO · Secbiz IT Security GmbH

- بنیان‌گذار و مدیر فنی یک شرکت امنیت سایبری.
- پژوهش و مشاوره در امنیت صنعتی/OT و برنامه‌های کاربردی.
- نمایش زنده حمله به SCADA در Hannover Messe 2019.

Veloce

Veloce ران‌تایم JavaScript/TypeScript من برای agentic coding است: یک پلتفرم هدف که عامل‌های کدنویسی می‌توانند روی آن برنامه‌های کامل، خوانا، قابل ممیزی و آماده اجرا تولید کنند، بدون اینکه ابتدا وابستگی‌های npm، فریم‌ورک‌ها، ابزارهای build و لایه‌های deployment را به هم متصل کنند.

ران‌تایم اجزای مهم را مستقیماً در خود دارد: sandbox محدودکننده و مدل مجوزها، سرور HTTP، SQLite و PostgreSQL همراه ORM و KV store، قابلیت‌های مرورگر و دسکتاپ و بسته‌بندی به یک native binary مستقل. مسیرهای محاسباتی سنگین را می‌توان از JavaScript/TypeScript به native kernelهای مبتنی بر Rust یا WebAssembly منتقل کرد. هدف نرم‌افزاری است که عامل‌ها بتوانند با اطمینان تولید کنند، انسان‌ها همچنان بفهمند و سیستم‌ها با کمترین قطعات متحرک اجرا کنند.

تخصص

سامانه‌های تعبیه‌شده، OT و تجهیزات پزشکی

پژوهش آسیب‌پذیری در firmware و دستگاه‌های متصل: سامانه‌های اعلام حریق، کنترل‌کننده‌های صنعتی (SCADA)، تجهیزات بیمارستانی و پزشکی.

توسعه exploit

از یک نقص memory corruption منفرد تا زنجیره کامل exploit با دسترسی root از راه دور.

امنیت مرورگر و وب

دور زدن SOP/CORS، مسیرهای حمله به دستگاه‌های شبکه داخلی، XSS و امنیت برنامه‌ها.

افشای مسئولانه

گزارش و هماهنگی با سازندگان و بهره‌برداران، از شرکت‌های بزرگ تا مدیریت‌های شهری، همراه با پشتیبانی در فرایند رفع مشکل.

ابزارهای اختصاصی

ابزار و خودکارسازی برای کشف آسیب‌پذیری و penetration testing، از جمله workflowهای کمک‌گرفته از AI. سازنده runtime جاوااسکریپت/تایپ‌اسکریپت Veloce.

پژوهش

سال	پژوهش / آسیب‌پذیری	منبع
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	مدخل CISA در CIRCL
2013	Apple Motion - CVE-2013-6114 - آسیب‌پذیری	Apple
2014	Apple Web Server - پژوهش امنیت, ۱۳۹۲ بهمن	Apple
2012	Nokia Hall of Fame - پژوهش امنیت, ۱۳۹۱ آذر	Nokia
2012	Android Browser DoS - CVE-2012-6301 - ماژول Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	آرشیو 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

رسانه

سال	مقاله اصلی	رسانه
2025	پوشش رسانه‌ای افشای مسئولانه در Securitas / Marvelit	Security-Insider
2022	برنامه‌ی رادیویی درباره‌ی امنیت سایبری و هک اخلاقی	WDR
2024	گفت‌وگوی کارشناسی ÖAG: امنیت ۴.۰ - امنیت سایبری و دفاع با هوش مصنوعی	medianet (اتریش)
2024	آسیب‌پذیری‌های امنیتی در بیمارستان‌ها: بیماران در معرض خطر	Golem
2024	SOP/CORS مرورگر و دستگاه‌های شبکه‌ی داخلی	CYTRES Research
2024	هشدار امنیتی عمومی Jean Pereira همراه با به‌روزرسانی مستند درباره‌ی رفع مشکل	Volksbank / Sparda Bank (Responsible Disclosure)
2023	گفت‌وگوی کارشناسی با دبیر دولتی تورسکی درباره‌ی دیجیتالی‌شدن، هوش مصنوعی و امنیت سایبری	KURIER (اتریش)
2023	حضور به‌عنوان کارشناس امنیت سایبری در ÖAG Super Tuesday	LEADERSNET (اتریش)
2022	پادکست #51: Ethical Hacker - پژوهش امنیت و مسیر حرفه‌ای	IDG TechTalk / COMPUTERWOCHE
2022	آسیب‌پذیری امنیت فناوری اطلاعات در شهرداری کلن	Kölner Stadt-Anzeiger
2022	کمیسر حفاظت از داده‌ها درباره نادیده گرفتن یک آسیب‌پذیری امنیتی گزارش‌شده تحقیق می‌کند	WirtschaftsWoche
2022	افشای مسئولانه / ۴۵ سازمان	Golem
2022	گزارش درباره‌ی OBI و نهادهای دولتی	connect professional
2020	سخنرانی اصلی درباره‌ی امنیت مرورگر و برنامه‌های کاربردی	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: هک زنده‌ی SCADA/ICS	Hannover Messe / MittelstandsWiki
2019	مصاحبه «به هکرهای بیشتری نیاز داریم»	atp magazin
2019	حملات سایبری و دارک‌نت - مصاحبه با Jean Pereira	"Podcast "IT'S IN YOU
2018	SEO-DAY: چگونه در سال ۲۰۱۸ Chrome را هک و SSL را دور بزنیم	Host Europe
2018	سخنرانی امنیتی در سوپرپنل SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker و بنیان‌گذار SECBIZ در فهرست سخنرانان	DSS IT SEC / Riga