Jean Pereira

Nghiên cứu bảo mật · Offensive security · Kỹ thuật full-stack

Tôi nghiên cứu lỗ hổng trong các hệ thống phức tạp và phát triển phần mềm bảo mật cùng các sản phẩm riêng trong lĩnh vực bảo mật trình duyệt, hệ thống nhúng và công nghiệp, tự động hóa và AI.

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

Hồ sơ

Tôi tìm ra lỗ hổng bảo mật ở nơi người khác ngừng tìm kiếm và xây dựng phần mềm an toàn để giải quyết những vấn đề phức tạp.

Công việc của tôi bao gồm các lỗ hổng trong sản phẩm và công nghệ của **Siemens**, **Apple**, **Google**, **Microsoft** và **Nokia**, cũng như các dự án khác nhau trong lĩnh vực công nghệ y tế. Hiện tôi tập trung vào nghiên cứu bảo mật và kỹ thuật phần mềm.

Tôi cũng là tác giả của **Veloce**. Bạn có thể liên hệ với tôi qua biểu mẫu liên hệ hoặc trực tiếp trên LinkedIn.

Điểm nổi bật

Bốn zero-day tại Siemens: hệ thống báo động và đầu báo cháy bị chiếm quyền từ xa

Tôi chiếm toàn quyền từ xa đối với hệ thống báo động và đầu báo cháy Siemens. Mã khai thác của tôi cấp quyền root, tức quyền hệ thống cao nhất, không cần thông tin đăng nhập, nhấp chuột hay bất kỳ tương tác nào của nạn nhân.

Tôi phát triển chuỗi khai thác kết hợp bốn lỗ hổng chưa được biết đến và chứng minh việc chiếm toàn quyền trong thực tế. Đây là quyền kiểm soát công nghệ báo động thiết yếu cho an toàn.

Siemens xác nhận bốn phát hiện từ CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Mã khai thác được đánh giá CVSS 10.0, mức nghiêm trọng tối đa có thể.

Zero-day trong bệnh viện: nhóm máu bị sửa, cảnh báo ECG và thiết bị thông gió bị tắt

Trong một đợt đánh giá, tôi phát hiện 22 lỗ hổng chưa được biết đến trong thiết bị của mười hai nhà sản xuất và trình diễn tấn công bằng mã khai thác hoạt động: tắt cảnh báo ECG, ngắt thông gió phòng mổ vô trùng và sửa nhóm máu, hồ sơ dị ứng. Tôi cũng phát triển kỹ thuật vượt SOP/CORS để chứng minh tấn công từ xa vào thiết bị nội bộ không thể truy cập trực tiếp từ internet.

Các nhà sản xuất được nghiên cứu gồm ZEISS, MOXA, Zebra, Dedalus Labor và Tetronik. Theo phóng sự Golem năm 2024, thiết bị liên quan được sử dụng tại hàng nghìn bệnh viện và cơ sở y tế khác. Tôi điều phối công bố cho nhà sản xuất và hỗ trợ khắc phục. Các nhà báo theo dõi toàn bộ quá trình, từ thông báo cho nhà sản xuất đến việc tôi hỗ trợ khắc phục.

Lỗ hổng tại hơn 40 cơ quan công quyền, OBI, REWE và Viện Fraunhofer

Tôi phát hiện lỗ hổng tại 45 chính quyền địa phương và doanh nghiệp, rồi báo cho các bên phụ trách. Tại OBI, một lỗ hổng web cho phép chiếm phiên người dùng và đọc thông tin từ hệ thống quản lý nội dung nội bộ.

Nhiều chính quyền đã khắc phục. OBI ngừng trang web liên quan sau tranh luận công khai. Golem và WirtschaftsWoche ghi nhận nghiên cứu và phản ứng của các doanh nghiệp.

Kinh nghiệm

thg 6 2023 - hiện tại

CEO · CTO · CYTRES GmbH
Thành lập và điều hành công ty, tập trung vào phát triển phần mềm và nghiên cứu an ninh mạng.

thg 12 2016 - thg 8 2019

Giảng viên an ninh mạng · CIC (Cambridge Innovation Center) · Rotterdam, Hà Lan
Tổ chức các hội thảo an ninh mạng và khóa đào tạo kỹ thuật.

thg 12 2016 - thg 8 2019

Cố vấn an ninh cao cấp · Base Cyber Security · Rotterdam, Hà Lan
Lãnh đạo đội ngũ kỹ thuật và đào tạo nhân viên mới đạt tiêu chuẩn kỹ thuật cần thiết.

2019

Nhà sáng lập · CEO · CTO · Secbiz IT Security GmbH

- Nhà sáng lập và lãnh đạo kỹ thuật một công ty an ninh mạng.
- Nghiên cứu và tư vấn bảo mật công nghiệp/OT và ứng dụng.
- Trình diễn tấn công SCADA trực tiếp tại Hannover Messe 2019.

Veloce

Veloce là runtime JavaScript/TypeScript của tôi dành cho agentic coding: một nền tảng đích nơi coding agent có thể tạo ra ứng dụng hoàn chỉnh, dễ đọc, có thể kiểm tra và chạy ngay, mà không phải ghép trước các dependency npm, framework, build tooling và deployment glue.

Runtime tích hợp sẵn các khối quan trọng: sandbox và mô hình permission hạn chế, HTTP server, SQLite và PostgreSQL với ORM và KV store, khả năng browser và desktop, cùng packaging thành một native binary độc lập. Các luồng tính toán nặng có thể được chuyển từ JavaScript/TypeScript sang native kernel dựa trên Rust hoặc WebAssembly. Mục tiêu là phần mềm mà agent có thể tạo ổn định, con người vẫn hiểu được và hệ thống có thể chạy với ít thành phần chuyển động nhất có thể.

Chuyên môn

Hệ thống nhúng, OT và thiết bị y tế

Nghiên cứu lỗ hổng trong firmware và thiết bị kết nối: hệ thống báo cháy, bộ điều khiển công nghiệp (SCADA), thiết bị bệnh viện và thiết bị y tế.

Phát triển exploit

Từ một lỗi memory corruption đơn lẻ đến exploit chain hoàn chỉnh với quyền root từ xa.

Bảo mật trình duyệt và web

Bypass SOP/CORS, đường tấn công tới thiết bị trong mạng nội bộ, XSS và bảo mật ứng dụng.

Công bố có trách nhiệm

Báo cáo và phối hợp với nhà sản xuất và đơn vị vận hành, từ tập đoàn lớn đến chính quyền đô thị, bao gồm hỗ trợ khắc phục.

Công cụ riêng

Tooling và tự động hóa cho phát hiện lỗ hổng và penetration testing, bao gồm workflow có hỗ trợ AI. Tác giả runtime JavaScript/TypeScript Veloce.

Nghiên cứu

Năm	Nghiên cứu / lỗ hổng	Nguồn
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	mục CISA tại CIRCL
2013	Apple Motion - CVE-2013-6114 - lỗ hổng bảo mật	Apple
2014	Apple Web Server - nghiên cứu bảo mật, tháng 2 năm 2014	Apple
2012	Nokia Hall of Fame - nghiên cứu bảo mật, tháng 12 năm 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - mô-đun Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	kho lưu trữ 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

Năm	Nghiên cứu / lỗ hổng	Nguồn
2012	plow .plowrc - Buffer Overflow - BID 54290	Bugtraq
2012	Internet Explorer - XSS Filter Bypass - Exploit-DB 22100	VulDB

Báo chí

Năm	Bài gốc	Báo chí
2025	Bài viết về quy trình công bố có trách nhiệm tại Securitas / Marvelit	Security-Insider
2022	Chương trình phát thanh về an ninh mạng và hacking có đạo đức	WDR
2024	Tọa đàm chuyên gia ÖAG: An ninh 4.0 - an ninh mạng và phòng thủ bằng AI	medianet (Áo)
2024	Lỗ hổng bảo mật trong bệnh viện: bệnh nhân gặp nguy hiểm	Golem
2024	SOP/CORS của trình duyệt và thiết bị mạng nội bộ	CYTRES Research
2024	Thông báo bảo mật công khai của Jean Pereira kèm cập nhật khắc phục được ghi nhận	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Tọa đàm với Quốc vụ khanh Tursky về số hóa, AI và an ninh mạng	KURIER (Áo)
2023	Tham gia ÖAG Super Tuesday với vai trò chuyên gia an ninh mạng	LEADERSNET (Áo)
2022	Podcast #51: Ethical Hacker - nghiên cứu bảo mật và hành trình nghề nghiệp	IDG TechTalk / COMPUTERWOCHE
2022	Lỗ hổng bảo mật CNTT tại chính quyền thành phố Köln	Kölner Stadt-Anzeiger
2022	Ủy viên bảo vệ dữ liệu điều tra sau khi một lỗ hổng bảo mật đã được báo cáo bị phớt lờ	WirtschaftsWoche
2022	Công bố có trách nhiệm / 45 tổ chức	Golem
2022	Bài viết về OBI và các cơ quan công quyền	connect professional
2020	Bài keynote về bảo mật trình duyệt và ứng dụng	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: hack SCADA/ICS trực tiếp	Hannover Messe / MittelstandsWiki
2019	Phỏng vấn "Chúng ta cần thêm nhiều hacker"	atp magazin
2019	Tấn công mạng & darknet - phỏng vấn Jean Pereira	Podcast "IT'S IN YOU"
2018	SEO-DAY: cách hack Chrome và vượt qua SSL năm 2018	Host Europe
2018	Bài nói chuyện về bảo mật trong superpanel SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker và nhà sáng lập SECBIZ trong danh sách diễn giả	DSS IT SEC / Riga