Jean Pereira

سیکیورٹی تحقیق · Offensive Security · Full-Stack Engineering

میں پیچیدہ نظاموں میں vulnerabilities پر تحقیق کرتا ہوں اور browser security، embedded اور industrial systems، automation اور AI کے لیے security software اور اپنے آزاد products تیار کرتا ہوں۔

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

تعارف

میں وہاں سیکیورٹی کمزوریاں تلاش کرتا ہوں جہاں دوسرے تلاش چھوڑ دیتے ہیں، اور ایسا محفوظ سافٹ ویئر بناتا ہوں جو پیچیدہ مسائل حل کرتا ہے۔

میرے کام میں **Microsoft**، **Google**، **Apple**، **Siemens** اور **Nokia** کی products اور technologies میں vulnerabilities کے ساتھ طبی ٹیکنالوجی کے مختلف منصوبے بھی شامل ہیں۔ اس وقت میری توجہ سیکیورٹی تحقیق اور سافٹ ویئر انجینئرنگ پر ہے۔

میں **Veloce** کا مصنف بھی ہوں۔ تم رابطے کے فارم کے ذریعے یا براہِ راست LinkedIn پر مجھ سے رابطہ کر سکتے ہو۔

نمایاں نکات

Siemens میں چار زیرو ڈیز: الارم سسٹمز اور فائر ڈیٹیکٹرز کا دور سے کنٹرول حاصل کیا

میں نے Siemens الارم سسٹمز اور فائر ڈیٹیکٹرز کا دور سے مکمل کنٹرول حاصل کیا۔ میرے ایکسپلائٹ نے root رسائی، یعنی اعلیٰ ترین سسٹم اختیارات دیے۔ لاگ اِن معلومات، کلک یا متاثرہ شخص کے کسی تعامل کی ضرورت نہیں تھی۔

میں نے چار نامعلوم کمزوریوں کو ملا کر ایکسپلائٹ چین تیار کی اور مکمل کنٹرول کا عملی مظاہرہ کیا۔ یہ حفاظت کے لیے انتہائی اہم الارم ٹیکنالوجی پر کنٹرول تھا۔

Siemens نے چاروں نتائج کی CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904 کے طور پر تصدیق کی۔ ایکسپلائٹ کو CVSS 10.0 ملا، یعنی زیادہ سے زیادہ ممکنہ شدت۔

ہسپتالوں میں زیرو ڈیز: بلڈ گروپ بدلے گئے، **ECG** الارم اور ہوا کی گردش کے آلات بند کیے گئے

ایک سیکیورٹی جائزے میں بارہ سازندگان کے آلات میں 22 نامعلوم کمزوریاں دریافت کیں اور حقیقی ایکسپلائٹس سے حملے دکھائے: ECG الارم بند کرنا، جراثیم سے پاک آپریشن تھیٹروں کی وینٹیلیشن روکنا اور بلڈ گروپ و الرجی کے ریکارڈ بدلنا۔ اپنے SOP/CORS بائی پاسز سے ایسے اندرونی آلات پر بھی ریموٹ حملے دکھائے جو انٹرنیٹ سے براہ راست قابل رسائی نہیں تھے۔

تحقیق میں ZEISS، MOXA، Zebra، Dedalus Labor اور Tetronik شامل تھے۔ Golem کی 2024 کی رپورٹ کے مطابق متعلقہ آلات ہزاروں دیگر ہسپتالوں اور طبی مراکز میں استعمال ہو رہے تھے۔ میں نے سازندگان کو اطلاع اور اصلاح میں تعاون کو مربوط کیا۔ صحافیوں نے سازندگان کو اطلاع دینے سے لے کر اصلاح میں میری معاونت تک پورے عمل کی پیروی کی۔

40 سے زیادہ سرکاری اداروں، **REWE**، **OBI** اور **Fraunhofer** انسٹی ٹیوٹ میں سیکیورٹی کمزوریاں

میں نے 45 بلدیاتی انتظامیہ اور کمپنیوں میں کمزوریاں دریافت کر کے ذمہ داروں کو اطلاع دی۔ OBI میں ایک ویب کمزوری سے صارف سیشن پر قبضہ اور اندرونی مواد کے انتظامی نظام سے معلومات پڑھنا ممکن تھا۔

کئی بلدیاتی اداروں نے خامیاں دور کیں۔ عوامی تنازع کے بعد OBI نے متعلقہ ویب سائٹ بند کر دی۔ Golem اور WirtschaftsWoche نے تحقیق اور کمپنیوں کے ردعمل کو دستاویزی شکل دی۔

تجربہ

جون 2023 - تاحال

CEO · CTO · CYTRES GmbH

سافٹ ویئر ڈیولپمنٹ اور سائبر سیکیورٹی تحقیق پر توجہ کے ساتھ کمپنی قائم کی اور اس کی قیادت کی۔

دسمبر 2016 - اگست 2019

سائبر سیکیورٹی ٹیوٹر · CIC (Cambridge Innovation Center) · Rotterdam, نیدر لینڈز

سائبر سیکیورٹی ورکشاپس اور تکنیکی تربیت منعقد کی۔

دسمبر 2016 - اگست 2019

سینئر سیکیورٹی ایڈوائزر · Base Cyber Security · Rotterdam, نیدر لینڈز

تکنیکی ٹیم کی قیادت کی اور نئے ملازمین کو مطلوبہ تکنیکی معیار تک تربیت دی۔

2019

بانی · CEO · CTO · Secbiz IT Security GmbH

- سائبر سیکیورٹی کمپنی کے بانی اور تکنیکی سربراہ۔
- صنعتی/OT اور ایپلیکیشن سیکیورٹی میں تحقیق و مشاورت۔
- Hannover Messe 2019 میں SCADA حملے کا براہِ راست مظاہرہ۔

Veloce

Veloce agentic coding کے لیے میرا JavaScript/TypeScript رن ٹائم ہے: ایک ایسا target platform جس پر coding agents مکمل applications بنا سکتے ہیں جو پڑھنے کے قابل، audit کیے جا سکیں اور فوراً چل سکیں، بغیر پہلے frameworks، npm dependencies، build tooling اور deployment glue جوڑنے کے۔

رن ٹائم اہم building blocks براہِ راست فراہم کرتا ہے: محدود sandbox اور ORM، HTTP server، permission model اور KV store کے ساتھ browser، SQLite/PostgreSQL، desktop capabilities اور standalone native binary میں packaging- بھاری computation کو JavaScript/TypeScript سے Rust-backed native kernels یا WebAssembly میں offload کیا جا سکتا ہے۔ مقصد ایسا software ہے جسے agents قابلِ اعتماد طریقے سے بنا سکیں، انسان سمجھتے رہیں اور systems کم سے کم moving parts کے ساتھ چلا سکیں۔

مہارت

Embedded, OT اور **medical devices**

Firmware اور connected devices میں، vulnerability research: fire alarm systems، industrial controllers (SCADA)، hospital اور medical equipment-

Exploit development

ایک memory-corruption bug سے remote root access والی مکمل exploit chain تک-

Browser اور **web security**

SOP/CORS bypasses، internal network devices تک XSS، attack paths اور application security-

Responsible disclosure

Vendors اور operators کے ساتھ reporting اور coordination، بڑی کمپنیوں سے municipal administrations تک، remediation support سمیت-

اپنے **tools**

Vulnerability discovery اور penetration testing کے لیے tooling اور AI-assisted workflows، automation سمیت- Veloce JavaScript/TypeScript runtime کا مصنف-

تحقیق

سال	تحقیق / کمزوری	ذریعہ
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	CIRCL پر CISA اندراج
2013	Apple Motion - CVE-2013-6114 - سیکیورٹی کمزوری	Apple
2014	Apple Web Server - سیکیورٹی تحقیق, فروری 2014	Apple
2012	Nokia Hall of Fame - سیکیورٹی تحقیق, دسمبر 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit ماڈیول	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq آرکائیو
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

میڈیا

سال	اصل مضمون	میڈیا
2025	Securitas / Marvelit میں ذمہ دارانہ انکشاف پر کوریج	Security-Insider
2022	سائبر سیکیورٹی اور اخلاقی ہیکنگ پر ریڈیو پروگرام	WDR
2024	ÖAG ماہرین کی گفتگو: سیکیورٹی 4.0 - سائبر سیکیورٹی اور AI پر مبنی دفاع	medianet (آسٹریا)
2024	ہسپتالوں میں سیکیورٹی کمزوریاں: مریض خطرے میں	Golem
2024	براؤزر SOP/CORS اور اندرونی نیٹ ورک ڈیوائسز	CYTRES Research
2024	Jean Pereira کی عوامی سیکیورٹی اطلاع، اصلاح کے دستاویزی اپ ڈیٹ کے ساتھ	Volksbank / Sparda Bank (Responsible Disclosure)
2023	ریاستی سیکریٹری ٹورسکی کے ساتھ ڈیجیٹلائزیشن، AI اور سائبر سیکیورٹی پر ماہرین کی گفتگو	KURIER (آسٹریا)
2023	ÖAG Super Tuesday میں سائبر سیکیورٹی ماہر کے طور پر شرکت	LEADERSNET (آسٹریا)
2022	پوڈکاسٹ #51: Ethical Hacker - سیکیورٹی تحقیق اور پیشہ ورانہ سفر	IDG TechTalk / COMPUTERWOCHE
2022	کولون شہر کی انتظامیہ میں IT سیکیورٹی کمزوری	Kölner Stadt-Anzeiger
2022	اطلاع دی گئی سیکیورٹی خامی نظر انداز کیے جانے پر ڈیٹا پروٹیکشن کمشنر تحقیقات کر رہی ہیں	WirtschaftsWoche
2022	ذمہ دارانہ انکشاف / 45 ادارے	Golem
2022	OBI اور سرکاری اداروں پر رپورٹ	connect professional
2020	براؤزر اور ایپلیکیشن سیکیورٹی پر کلیدی خطاب	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: لائیو SCADA/ICS ہیکنگ	Hannover Messe / MittelstandsWiki
2019	انٹرویو "ہمیں مزید ہیکرز کی ضرورت ہے"	atp magazin
2019	سائبر حملے اور ڈارک نیٹ - Jean Pereira کے ساتھ انٹرویو	"Podcast "IT'S IN YOU
2018	SEO-DAY: 2018 میں Chrome کو ہیک اور SSL کو بائی پاس کرنے کا طریقہ	Host Europe
2018	SEO-DAY 2018 کے سپر پینل میں سیکیورٹی لیکچر	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker اور SECBIZ کے بانی مقررین کی فہرست میں	DSS IT SEC / Riga