Jean Pereira

सुरक्षा अनुसंधान · Offensive Security · Full-Stack Engineering

मैं जटिल प्रणालियों में vulnerabilities पर शोध करता हूँ और browser security, embedded तथा industrial systems, automation और AI के क्षेत्र में security software और अपने स्वतंत्र products विकसित करता हूँ।

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

प्रोफ़ाइल

मैं वहाँ सुरक्षा कमज़ोरियाँ ढूँढता हूँ जहाँ दूसरे तलाश बंद कर देते हैं, और ऐसा सुरक्षित सॉफ्टवेयर बनाता हूँ जो जटिल समस्याएँ हल करता है।

मेरे काम में **Siemens**, **Apple**, **Google**, **Microsoft** और **Nokia** के products और technologies में vulnerabilities के साथ चिकित्सा प्रौद्योगिकी में विभिन्न परियोजनाएँ भी शामिल हैं। वर्तमान में मेरा ध्यान सुरक्षा अनुसंधान और सॉफ्टवेयर इंजीनियरिंग पर है।

मैं **Veloce** का लेखक भी हूँ। तुम संपर्क फ़ॉर्म के ज़रिए या सीधे LinkedIn पर मुझसे संपर्क कर सकते हो।

प्रमुख बिंदु

Siemens में चार ज़ीरो-डे: अलार्म प्रणालियों और अग्नि डिटेक्टरों का दूर से नियंत्रण हासिल किया

मैंने Siemens अलार्म प्रणालियों और अग्नि डिटेक्टरों का दूर से पूरा नियंत्रण हासिल किया। मेरे एक्सप्लॉइट ने root पहुँच, यानी सर्वोच्च सिस्टम अधिकार दिए। इसके लिए लॉगिन जानकारी, क्लिक या पीड़ित की किसी भी भागीदारी की आवश्यकता नहीं थी।

मैंने चार अज्ञात कमज़ोरियों को जोड़कर एक्सप्लॉइट चेन विकसित की और पूरा नियंत्रण व्यावहारिक रूप से साबित किया। यह सुरक्षा के लिए अत्यंत महत्वपूर्ण अलार्म तकनीक पर नियंत्रण था।

Siemens ने चारों खोजों की पुष्टि CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904 के रूप में की। एक्सप्लॉइट को CVSS 10.0 मिला, यानी अधिकतम संभव गंभीरता।

अस्पतालों में ज़ीरो-डे: रक्त समूह बदले, **ECG** अलार्म और वायु संचार उपकरण बंद किए

एक सुरक्षा आकलन में मैंने बारह निर्माताओं की उपकरणों में 22 अज्ञात कमज़ोरियाँ खोजीं और कार्यशील एक्सप्लॉइट से हमले प्रदर्शित किए: ECG अलार्म बंद करना, स्टेराइल ऑपरेशन थिएटर की वेंटिलेशन रोकना तथा रक्त समूह और एलर्जी के रिकॉर्ड बदलना। अपने SOP/CORS बायपास से उन आंतरिक उपकरणों पर भी रिमोट हमले दिखाए जो इंटरनेट से सीधे उपलब्ध नहीं थे।

जाँचे गए निर्माताओं में ZEISS, MOXA, Zebra, Dedalus Labor और Tetronik शामिल हैं। Golem की 2024 की रिपोर्ट के अनुसार ऐसे उपकरण हज़ारों अन्य अस्पतालों और चिकित्सा संस्थानों में उपयोग होते थे। मैंने निर्माताओं को सूचना देने और सुधार में सहयोग का समन्वय किया। पत्रकारों ने निर्माताओं को सूचना देने से लेकर सुधार में मेरे सहयोग तक पूरी प्रक्रिया को कवर किया।

40 से अधिक सरकारी संस्थाओं, **OBI**, **REWE** और **Fraunhofer** संस्थान में सुरक्षा कमज़ोरियाँ

मैंने 45 नगर प्रशासन और कंपनियों में कमज़ोरियाँ खोजीं और जिम्मेदार टीमों को सूचित किया। OBI में एक वेब कमज़ोरी से उपयोगकर्ता सत्रों पर कब्ज़ा और आंतरिक सामग्री प्रबंधन प्रणाली से जानकारी पढ़ना संभव था।

कई नगर प्रशासनों ने समस्याएँ ठीक कीं। सार्वजनिक विवाद के बाद OBI ने संबंधित वेबसाइट बंद कर दी। Golem और WirtschaftsWoche ने शोध और कंपनियों की प्रतिक्रियाओं को दर्ज किया।

अनुभव

जून 2023 - वर्तमान

CEO · CTO · CYTRES GmbH
सॉफ्टवेयर विकास और साइबर सुरक्षा अनुसंधान पर ध्यान देते हुए कंपनी की स्थापना और नेतृत्व किया।

दिस॰ 2016 - अग॰ 2019

साइबर सुरक्षा ट्यूटर · CIC (Cambridge Innovation Center) · Rotterdam, नीदरलैंड
साइबर सुरक्षा कार्यशालाएँ और तकनीकी प्रशिक्षण आयोजित किए।

दिस॰ 2016 - अग॰ 2019

वरिष्ठ सुरक्षा सलाहकार · Base Cyber Security · Rotterdam, नीदरलैंड
तकनीकी टीम का नेतृत्व किया और नए कर्मचारियों को आवश्यक तकनीकी स्तर तक प्रशिक्षित किया।

2019

संस्थापक · **CEO** · **CTO** · Secbiz IT Security GmbH
- साइबर सुरक्षा कंपनी के संस्थापक और तकनीकी प्रमुख।
- औद्योगिक/OT और एप्लिकेशन सुरक्षा में अनुसंधान और परामर्श।
- Hannover Messe 2019 में SCADA हैकिंग का लाइव प्रदर्शन।

Veloce

Veloce agentic coding के लिए मेरा JavaScript/TypeScript runtime है: एक target platform जिस पर coding agents पूर्ण applications बना सकते हैं जो पढ़ने योग्य, audit करने योग्य और सीधे चलने योग्य हों - बिना पहले npm dependencies, frameworks, build tooling और deployment glue जोड़ने के।

Runtime जरूरी building blocks को सीधे शामिल करता है: restrictive sandbox और permission model, HTTP server, ORM और KV store के साथ SQLite/PostgreSQL, browser और desktop capabilities, और standalone native binary में packaging। Compute-heavy paths को JavaScript/TypeScript से Rust-backed native kernels या WebAssembly में offload किया जा सकता है। लक्ष्य ऐसा software है जिसे agents भरोसेमंद तरीके से बना सकें, इंसान समझते रहें और systems कम से कम moving parts के साथ चला सकें।

विशेषज्ञता

Embedded, OT और medical devices

Firmware और connected devices में vulnerability research: fire alarm systems, industrial controllers (SCADA), hospital और medical equipment।

Exploit development

एक memory-corruption bug से लेकर remote root access वाली पूरी exploit chain तक।

Browser और web security

SOP/CORS bypasses, internal network devices तक attack paths, XSS और application security।

Responsible disclosure

Vendors और operators के साथ reporting और coordination, बड़े corporations से municipalities तक, remediation support सहित।

अपने tools

Vulnerability discovery और penetration testing के लिए tooling और automation, AI-assisted workflows सहित। Veloce JavaScript/TypeScript runtime का लेखक।

अनुसंधान

वर्ष	शोध / भेद्यता	स्रोत
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 पर CISA प्रविष्टि
2013	Apple Motion - CVE-2013-6114 - सुरक्षा कमजोरी	Apple
2014	Apple Web Server - सुरक्षा अनुसंधान, फ़रवरी 2014	Apple
2012	Nokia Hall of Fame - सुरक्षा अनुसंधान, दिसंबर 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit मॉड्यूल	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq अभिलेख
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

मीडिया

वर्ष	मूल लेख	मीडिया
2025	Securitas / Marvelit में जिम्मेदार प्रकटीकरण पर कवरेज	Security-Insider
2022	साइबर सुरक्षा और एथिकल हैकिंग पर रेडियो कार्यक्रम	WDR
2024	ÖAG विशेषज्ञ चर्चा: सुरक्षा 4.0 - साइबर सुरक्षा और AI-आधारित रक्षा	medianet (ऑस्ट्रिया)
2024	अस्पतालों में सुरक्षा कमजोरियाँ: मरीज जोखिम में	Golem
2024	ब्राउज़र SOP/CORS और आंतरिक नेटवर्क उपकरण	CYTRES Research
2024	Jean Pereira की सार्वजनिक सुरक्षा सूचना, समाधान पर दस्तावेज़ित अपडेट के साथ	Volksbank / Sparda Bank (Responsible Disclosure)
2023	राज्य सचिव टर्स्की के साथ डिजिटलीकरण, AI और साइबर सुरक्षा पर विशेषज्ञ चर्चा	KURIER (ऑस्ट्रिया)
2023	ÖAG Super Tuesday में साइबर सुरक्षा विशेषज्ञ के रूप में भागीदारी	LEADERSNET (ऑस्ट्रिया)
2022	पॉडकास्ट #51: Ethical Hacker - सुरक्षा अनुसंधान और करियर यात्रा	IDG TechTalk / COMPUTERWOCHE
2022	कोलोन नगर प्रशासन में IT सुरक्षा कमजोरी	Kölner Stadt-Anzeiger
2022	रिपोर्ट की गई सुरक्षा खामी को अनदेखा किए जाने पर डेटा संरक्षण आयुक्त जाँच कर रही हैं	WirtschaftsWoche
2022	जिम्मेदार प्रकटीकरण / 45 संगठन	Golem
2022	OBI और सरकारी संस्थाओं पर रिपोर्ट	connect professional
2020	ब्राउज़र और एप्लिकेशन सुरक्षा पर मुख्य वक्तव्य	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: लाइव SCADA/ICS हैकिंग	Hannover Messe / MittelstandsWiki
2019	साक्षात्कार "हमें और हैकर चाहिए"	atp magazin
2019	साइबर हमले और डार्कनेट - Jean Pereira के साथ साक्षात्कार	Podcast "IT'S IN YOU"
2018	SEO-DAY: 2018 में Chrome को हैक और SSL को बायपास कैसे करें	Host Europe
2018	SEO-DAY 2018 के सुपरपैनल में सुरक्षा व्याख्यान	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker और SECBIZ संस्थापक वक्ताओं की सूची में	DSS IT SEC / Riga