Jean Pereira

Security Research · Offensive Security · Full-Stack Engineering

I research vulnerabilities in complex systems and build security software and independent products across browser security, embedded and industrial systems, automation, and AI.

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

Profile

I find security vulnerabilities where others stop looking and build secure software that solves complex problems.

My work includes vulnerabilities in products and technologies from **Siemens**, **Apple**, **Google**, **Microsoft**, and **Nokia**, as well as various projects in medical technology. My current focus is on security research and software engineering.

I am also the author of **Veloce**. You can reach me through the contact form or directly on LinkedIn.

Highlights

Four zero-days at Siemens: alarm systems and fire detectors taken over remotely

I remotely took full control of Siemens alarm systems and fire detectors. My own working exploit gave me the highest system privileges on the devices. No credentials, clicks or other victim interaction were required.

I discovered four previously unknown vulnerabilities and combined them into a working attack chain. The resulting root access let me execute my own code at operating-system level and fully control the devices. I demonstrated this takeover in practice.

Siemens confirmed my research in its own security advisory. The exploit received CVSS 10.0, the maximum possible severity. The four findings are documented as CVE-2024-47901, CVE-2024-47902, CVE-2024-47903 and CVE-2024-47904.

Hospital zero-days: blood groups manipulated, ECG alarms and ventilation units disabled

During a security assessment, I discovered 22 previously unknown vulnerabilities in devices from 12 manufacturers and demonstrated the attacks with working exploits: disabling ECG alarms, interrupting sterile operating-room ventilation, and manipulating blood groups and allergy records. I also developed SOP/CORS bypasses to demonstrate remote attacks against internal devices that were not directly reachable from the internet.

Manufacturers investigated include ZEISS, MOXA, Zebra, Dedalus Labor and Tetronik. Golem reported in 2024 that the affected devices were deployed in thousands of other hospitals and medical facilities. I coordinated vendor disclosure and supported remediation. Journalists followed the entire process, from disclosure to the manufacturers through my support for their remediation work.

Vulnerabilities at over 40 public authorities, OBI, REWE and the Fraunhofer Institute

I uncovered vulnerabilities at 45 municipalities and companies and reported them to the responsible teams. At OBI, a web vulnerability allowed user-session hijacking and access to information in the internal content management system.

Many affected municipalities fixed the reported flaws. OBI took the affected website offline after the public dispute. Golem and WirtschaftsWoche documented the research and how the companies handled the findings.

Experience

Jun 2023 - present

CEO · CTO · CYTRES GmbH
Founded and led the company with a focus on software development and cybersecurity research.

Dec 2016 - Aug 2019

Academic Tutor · CIC (Cambridge Innovation Center) · Rotterdam, Netherlands
Conducted cybersecurity workshops and technical training courses.

Dec 2016 - Aug 2019

Senior Security Advisor · Base Cyber Security · Rotterdam, Netherlands
Led the technical team and trained new employees to the required technical standard.

2019

Founder · CEO · CTO · Secbiz IT Security GmbH

- Founded and technically led a security company, providing security research, consulting and penetration testing.
- Focused on industrial/OT security, web and application security, and vulnerability assessment.
- Presented a live industrial SCADA hacking demonstration at Hannover Messe in 2019.

Veloce

Veloce is my JavaScript/TypeScript runtime for agentic coding: a target platform where coding agents can produce complete applications that are readable, auditable and immediately runnable - without first assembling npm dependencies, frameworks, build tooling and deployment glue.

The runtime ships the important building blocks as part of the platform: a restrictive sandbox and permission model, HTTP serving, SQLite and PostgreSQL with an ORM and KV store, browser and desktop capabilities, and packaging into a standalone native binary. Performance-sensitive paths can be offloaded from JavaScript/TypeScript to Rust-backed native kernels or WebAssembly. The goal is software that agents can generate reliably, humans can still understand, and systems can run with as few moving parts as possible.

Expertise

Embedded, OT & medical devices

Vulnerability research in firmware and connected devices: fire alarm systems, industrial controllers (SCADA), hospital and medical equipment.

Exploit development

From a single memory-corruption bug to a full exploit chain with remote root access.

Browser & web security

SOP/CORS bypasses, attack paths to devices on internal networks, XSS and application security.

Responsible disclosure

Reporting and coordinating with vendors and operators, from large corporations to municipalities, including support with remediation.

Own tooling

Tooling and automation for vulnerability discovery and penetration testing, including AI-assisted workflows. Author of the Veloce JavaScript/TypeScript runtime.

Research

Year	Research / vulnerability	Evidence
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 entry at CIRCL
2013	Apple Motion - CVE-2013-6114 - vulnerability	Apple
2014	Apple Web Server - security research, February 2014	Apple
2012	Nokia Hall of Fame - security research, December 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit module	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq archive
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

Year	Research / vulnerability	Evidence
2012	plow .plowrc - Buffer Overflow - BID 54290	Bugtraq
2012	Internet Explorer - XSS Filter Bypass - Exploit-DB 22100	VulDB

Press

Year	Original publication	Publisher
2025	Coverage of responsible disclosure at Securitas / Marvelit	Security-Insider
2022	Radio segment on cybersecurity and ethical hacking	WDR
2024	ÖAG expert talk: Security 4.0 - cybersecurity and AI defense	medianet (Austria)
2024	Security vulnerabilities in hospitals: patients at risk	Golem
2024	Browser SOP/CORS and internal network devices	CYTRES Research
2024	Public security notice by Jean Pereira with documented remediation update	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Expert talk with State Secretary Tursky on digitalization, AI and cybersecurity	KURIER (Austria)
2023	Joined the ÖAG Super Tuesday as a cybersecurity expert	LEADERSNET (Austria)
2022	Podcast #51: Ethical Hacker - security research and career path	IDG TechTalk / COMPUTERWOCHE
2022	IT security vulnerability at the City of Cologne	Kölner Stadt-Anzeiger
2022	Data protection commissioner investigates after a reported security vulnerability was ignored	WirtschaftsWoche
2022	Responsible disclosure / 45 organizations	Golem
2022	Report on OBI and public authorities	connect professional
2020	Keynote on browser and application security	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: live SCADA/ICS hacking	Hannover Messe / MittelstandsWiki
2019	Interview "We need more hackers"	atp magazin
2019	Cyberattacks & darknet - Jean Pereira in interview	Podcast "IT'S IN YOU"
2018	SEO-DAY: How to hack Chrome and bypass SSL in 2018	Host Europe
2018	Security talk in the SEO-DAY 2018 superpanel	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker and SECBIZ founder in the speaker line-up	DSS IT SEC / Riga