Jean Pereira

Riset keamanan · Offensive security · Rekayasa full-stack

Saya meneliti kerentanan dalam sistem kompleks dan mengembangkan perangkat lunak keamanan serta produk mandiri di bidang keamanan browser, sistem embedded dan industri, otomasi, dan AI.

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

Profil

Saya menemukan celah keamanan di tempat orang lain berhenti mencari dan membangun perangkat lunak aman yang memecahkan masalah kompleks.

Pekerjaan saya mencakup kerentanan dalam produk dan teknologi **Siemens**, **Apple**, **Google**, **Microsoft**, dan **Nokia**, serta berbagai proyek di bidang teknologi medis. Saat ini saya berfokus pada riset keamanan dan rekayasa perangkat lunak.

Saya juga pembuat **Veloce**. Kamu bisa menghubungi saya melalui formulir kontak atau langsung di LinkedIn.

Sorotan

Empat zero-day di Siemens: sistem alarm dan detektor kebakaran diambil alih dari jauh

Saya mengambil alih sepenuhnya sistem alarm dan detektor kebakaran Siemens dari jarak jauh. Exploit saya memberi akses root, hak sistem tertinggi, tanpa kredensial, klik atau interaksi korban lainnya.

Saya mengembangkan rantai exploit yang menggabungkan empat kerentanan tidak dikenal dan membuktikan pengambilalihan penuh dalam praktik. Ini berarti kendali atas teknologi alarm yang sangat penting bagi keselamatan.

Siemens mengonfirmasi keempat temuan sebagai CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Exploit tersebut mendapat nilai CVSS 10.0, tingkat keparahan maksimum yang mungkin.

Zero-day di rumah sakit: golongan darah dimanipulasi, alarm ECG dan perangkat ventilasi ruangan dimatikan

Dalam penilaian keamanan, saya menemukan 22 kerentanan yang belum dikenal pada perangkat dari dua belas produsen dan mendemonstrasikan serangan dengan exploit yang berfungsi: mematikan alarm ECG, menghentikan ventilasi ruang operasi steril, serta memanipulasi golongan darah dan catatan alergi. Saya juga mengembangkan bypass SOP/CORS untuk menunjukkan serangan jarak jauh terhadap perangkat internal yang tidak dapat diakses langsung dari internet.

Produsen yang diteliti mencakup ZEISS, MOXA, Zebra, Dedalus Labor dan Tetronik. Menurut laporan Golem tahun 2024, perangkat terkait digunakan di ribuan rumah sakit dan fasilitas medis lainnya. Saya mengoordinasikan pengungkapan kepada vendor dan mendukung perbaikan. Jurnalis mengikuti seluruh proses, dari pelaporan kepada produsen hingga dukungan saya untuk perbaikan.

Kerentanan di lebih dari 40 instansi pemerintah, OBI, REWE dan Institut Fraunhofer

Saya menemukan kerentanan di 45 pemerintah kota dan perusahaan serta melaporkannya kepada penanggung jawab. Di OBI, kerentanan web memungkinkan pembajakan sesi pengguna dan pembacaan informasi dari sistem manajemen konten internal.

Banyak pemerintah kota memperbaiki masalahnya. OBI menonaktifkan situs terkait setelah perselisihan publik. Golem dan WirtschaftsWoche mendokumentasikan riset serta tanggapan perusahaan.

Pengalaman

Jun 2023 - sekarang

CEO · CTO · CYTRES GmbH
Mendirikan dan memimpin perusahaan dengan fokus pada pengembangan perangkat lunak dan riset keamanan siber.

Des 2016 - Agu 2019

Tutor keamanan siber · CIC (Cambridge Innovation Center) · Rotterdam, Belanda
Menyelenggarakan lokakarya keamanan siber dan pelatihan teknis.

Des 2016 - Agu 2019

Penasihat keamanan senior · Base Cyber Security · Rotterdam, Belanda
Memimpin tim teknis dan melatih karyawan baru hingga mencapai standar teknis yang diperlukan.

2019

Pendiri · CEO · CTO · Secbiz IT Security GmbH
- Pendiri dan pemimpin teknis perusahaan keamanan siber.
- Riset dan konsultasi keamanan industri/OT dan aplikasi.
- Demonstrasi langsung serangan SCADA di Hannover Messe 2019.

Veloce

Veloce adalah runtime JavaScript/TypeScript saya untuk agentic coding: platform target tempat coding agent dapat membuat aplikasi lengkap yang mudah dibaca, dapat diaudit, dan langsung dijalankan tanpa harus lebih dulu merangkai dependensi npm, framework, build tooling, dan deployment glue.

Runtime ini menyediakan komponen penting secara terintegrasi: sandbox dan model permission yang ketat, server HTTP, SQLite dan PostgreSQL dengan ORM dan KV store, kemampuan browser dan desktop, serta packaging menjadi native binary mandiri. Jalur komputasi berat dapat dipindahkan dari JavaScript/TypeScript ke native kernel berbasis Rust atau WebAssembly. Tujuannya adalah software yang dapat dihasilkan agent secara andal, tetap dapat dipahami manusia, dan dijalankan sistem dengan sesedikit mungkin bagian yang bergerak.

Keahlian

Embedded, OT dan perangkat medis

Riset kerentanan pada firmware dan perangkat terhubung: sistem alarm kebakaran, pengendali industri (SCADA), peralatan rumah sakit dan perangkat medis.

Pengembangan exploit

Dari satu bug memory corruption hingga exploit chain lengkap dengan akses root jarak jauh.

Keamanan browser dan web

Bypass SOP/CORS, jalur serangan ke perangkat di jaringan internal, XSS, dan keamanan aplikasi.

Pengungkapan bertanggung jawab

Pelaporan dan koordinasi dengan vendor dan operator, dari perusahaan besar hingga pemerintah kota, termasuk dukungan remediasi.

Tooling sendiri

Tooling dan otomasi untuk penemuan kerentanan dan penetration testing, termasuk workflow berbantuan AI. Pembuat runtime JavaScript/TypeScript Veloce.

Riset

Tahun	Riset / kerentanan	Sumber
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	entri CISA di CIRCL
2013	Apple Motion - CVE-2013-6114 - kerentanan	Apple
2014	Apple Web Server - riset keamanan, Februari 2014	Apple
2012	Nokia Hall of Fame - riset keamanan, Desember 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - modul Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	arsip 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

Tahun	Riset / kerentanan	Sumber
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

Media

Tahun	Artikel asli	Media
2025	Liputan mengenai responsible disclosure di Securitas / Marvelit	Security-Insider
2022	Siaran radio tentang keamanan siber dan ethical hacking	WDR
2024	Diskusi pakar ÖAG: Keamanan 4.0 - keamanan siber dan pertahanan berbasis AI	medianet (Austria)
2024	Kerentanan keamanan di rumah sakit: pasien dalam bahaya	Golem
2024	SOP/CORS browser dan perangkat jaringan internal	CYTRES Research
2024	Pemberitahuan keamanan publik dari Jean Pereira dengan pembaruan perbaikan yang terdokumentasi	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Diskusi pakar bersama Sekretaris Negara Tursky tentang digitalisasi, AI, dan keamanan siber	KURIER (Austria)
2023	Berpartisipasi sebagai pakar keamanan siber di ÖAG Super Tuesday	LEADERSNET (Austria)
2022	Podcast #51: Ethical Hacker - riset keamanan dan perjalanan karier	IDG TechTalk / COMPUTERWOCHE
2022	Kerentanan keamanan TI di Pemerintah Kota Köln	Kölner Stadt-Anzeiger
2022	Komisioner perlindungan data menyelidiki kerentanan keamanan yang telah dilaporkan tetapi diabaikan	WirtschaftsWoche
2022	Responsible disclosure / 45 organisasi	Golem
2022	Liputan tentang OBI dan instansi pemerintah	connect professional
2020	Keynote tentang keamanan browser dan aplikasi	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: live hacking SCADA/ICS	Hannover Messe / MittelstandsWiki
2019	Wawancara "Kita membutuhkan lebih banyak hacker"	atp magazin
2019	Serangan siber & darknet - wawancara dengan Jean Pereira	Podcast "IT'S IN YOU"
2018	SEO-DAY: cara meretas Chrome dan melewati SSL pada 2018	Host Europe
2018	Presentasi keamanan di superpanel SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker dan pendiri SECBIZ dalam jajaran pembicara	DSS IT SEC / Riga