Jean Pereira

Penyelidikan keselamatan · Offensive security · Kejuruteraan full-stack

Saya menyelidik kerentanan dalam sistem kompleks dan membangunkan perisian keselamatan serta produk sendiri dalam keselamatan pelayar, sistem embedded dan industri, automasi dan AI.

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

Profil

Saya menemui kelemahan keselamatan di tempat orang lain berhenti mencari dan membina perisian selamat yang menyelesaikan masalah kompleks.

Kerja saya merangkumi kerentanan dalam produk dan teknologi **Siemens**, **Apple**, **Google**, **Microsoft** dan **Nokia**, serta pelbagai projek dalam teknologi perubatan. Fokus saya kini ialah penyelidikan keselamatan dan kejuruteraan perisian.

Saya juga pencipta **Veloce**. Kamu boleh menghubungi saya melalui borang hubungan atau terus di LinkedIn.

Sorotan

Empat zero-day di Siemens: sistem penggera dan pengesan kebakaran diambil alih dari jauh

Saya mengambil alih sepenuhnya sistem penggera dan pengesan kebakaran Siemens dari jauh. Exploit saya memberikan akses root, hak sistem tertinggi, tanpa kelayakan log masuk, klik atau interaksi mangsa yang lain.

Saya membangunkan rantaian exploit yang menggabungkan empat kelemahan tidak diketahui dan membuktikan pengambilalihan penuh secara praktikal. Ini bermakna kawalan terhadap teknologi penggera yang kritikal untuk keselamatan.

Siemens mengesahkan empat penemuan sebagai CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Exploit tersebut menerima penarafan CVSS 10.0, tahap keterukan maksimum yang mungkin.

Zero-day di hospital: kumpulan darah diubah, penggera ECG dan peralatan pengudaraan dimatikan

Dalam penilaian keselamatan, saya menemui 22 kelemahan yang belum diketahui dalam peranti daripada dua belas pengeluar dan menunjukkan serangan dengan exploit yang berfungsi: mematikan penggera ECG, menghentikan pengudaraan bilik bedah steril serta mengubah kumpulan darah dan rekod alahan. Saya turut membangunkan pintasan SOP/CORS untuk menunjukkan serangan jauh terhadap peranti dalaman yang tidak boleh dicapai terus melalui internet.

Pengeluar yang dikaji termasuk ZEISS, MOXA, Zebra, Dedalus Labor dan Tetronik. Menurut laporan Golem pada 2024, peranti berkenaan digunakan di ribuan hospital dan institusi perubatan lain. Saya menyelaraskan pendedahan kepada pengeluar dan menyokong pembaikan. Wartawan mengikuti keseluruhan proses, daripada pelaporan kepada pengeluar hingga sokongan saya untuk pembaikan.

Kelemahan di lebih 40 agensi kerajaan, OBI, REWE dan Institut Fraunhofer

Saya menemui kelemahan di 45 pihak berkuasa tempatan dan syarikat serta melaporkannya kepada pihak bertanggungjawab. Di OBI, kelemahan web membolehkan rampasan sesi pengguna dan pembacaan maklumat daripada sistem pengurusan kandungan dalaman.

Banyak pihak berkuasa membaiki masalah itu. OBI menutup laman terlibat selepas pertikaian awam. Golem dan WirtschaftsWoche mendokumentasikan kajian serta tindak balas syarikat.

Pengalaman

Jun 2023 - kini

CEO · CTO · CYTRES GmbH
Menubuhkan dan memimpin syarikat dengan fokus pada pembangunan perisian dan penyelidikan keselamatan siber.

Dis 2016 - Ogo 2019

Tutor keselamatan siber · CIC (Cambridge Innovation Center) · Rotterdam, Belanda
Mengendalikan bengkel keselamatan siber dan latihan teknikal.

Dis 2016 - Ogo 2019

Penasihat keselamatan kanan · Base Cyber Security · Rotterdam, Belanda
Memimpin pasukan teknikal dan melatih kakitangan baharu sehingga mencapai standard teknikal yang diperlukan.

2019

Pengasas · CEO · CTO · Secbiz IT Security GmbH
- Pengasas dan ketua teknikal sebuah syarikat keselamatan siber.
- Penyelidikan serta perundingan keselamatan industri/OT dan aplikasi.
- Demonstrasi serangan SCADA secara langsung di Hannover Messe 2019.

Veloce

Veloce ialah runtime JavaScript/TypeScript saya untuk agentic coding: platform sasaran tempat coding agent boleh menghasilkan aplikasi lengkap yang mudah dibaca, boleh diaudit dan terus boleh dijalankan tanpa perlu terlebih dahulu menyusun dependency npm, framework, build tooling dan deployment glue.

Runtime ini menyediakan komponen penting secara terbina dalam: sandbox dan model permission yang ketat, pelayan HTTP, SQLite dan PostgreSQL dengan ORM dan KV store, keupayaan browser dan desktop serta packaging menjadi native binary kendiri. Laluan pengiraan berat boleh dipindahkan daripada JavaScript/TypeScript kepada native kernel berasaskan Rust atau WebAssembly. Matlamatnya ialah software yang boleh dijana agent dengan boleh dipercayai, masih boleh difahami manusia dan boleh dijalankan sistem dengan sesedikit mungkin bahagian bergerak.

Kepakaran

Embedded, OT dan peranti perubatan

Penyelidikan kerentanan dalam firmware dan peranti bersambung: sistem penggera kebakaran, pengawal industri (SCADA), peralatan hospital dan peranti perubatan.

Pembangunan exploit

Daripada satu bug memory corruption kepada exploit chain lengkap dengan akses root dari jauh.

Keselamatan pelayar dan web

Bypass SOP/CORS, laluan serangan ke peranti dalam rangkaian dalaman, XSS dan keselamatan aplikasi.

Pendedahan bertanggungjawab

Pelaporan dan penyelarasan dengan pengeluar dan operator, daripada syarikat besar hingga pentadbiran perbandaran, termasuk sokongan pembaikan.

Tooling sendiri

Tooling dan automasi untuk penemuan kerentanan dan penetration testing, termasuk workflow berbantukan AI. Pencipta runtime JavaScript/TypeScript Veloce.

Penyelidikan

Tahun	Kajian / 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 - penyelidikan keselamatan, Februari 2014	Apple
2012	Nokia Hall of Fame - penyelidikan keselamatan, Disember 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - modul Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	arkib 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

Tahun	Kajian / kerentanan	Sumber
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

Media

Tahun	Artikel asal	Media
2025	Liputan mengenai pendedahan bertanggungjawab di Securitas / Marvelit	Security-Insider
2022	Siaran radio mengenai keselamatan siber dan penggodaman beretika	WDR
2024	Perbincangan pakar ÖAG: Keselamatan 4.0 - keselamatan siber dan pertahanan berasaskan AI	medianet (Austria)
2024	Kerentanan keselamatan di hospital: pesakit berisiko	Golem
2024	SOP/CORS pelayar dan peranti rangkaian dalaman	CYTRES Research
2024	Notis keselamatan awam oleh Jean Pereira dengan kemas kini pembaikan yang didokumenkan	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Perbincangan pakar bersama Setiausaha Negara Tursky mengenai pendigitalan, AI dan keselamatan siber	KURIER (Austria)
2023	Penyertaan sebagai pakar keselamatan siber di ÖAG Super Tuesday	LEADERSNET (Austria)
2022	Podcast #51: Ethical Hacker - penyelidikan keselamatan dan perjalanan kerjaya	IDG TechTalk / COMPUTERWOCHE
2022	Kerentanan keselamatan IT di bandar Köln	Kölner Stadt-Anzeiger
2022	Pesuruhjaya perlindungan data menyiasat kelemahan keselamatan yang dilaporkan tetapi diabaikan	WirtschaftsWoche
2022	Pendedahan bertanggungjawab / 45 organisasi	Golem
2022	Laporan mengenai OBI dan pihak berkuasa awam	connect professional
2020	Keynote mengenai keselamatan pelayar dan aplikasi	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: penggodaman SCADA/ICS secara langsung	Hannover Messe / MittelstandsWiki
2019	Temu bual "Kita memerlukan lebih ramai penggodam"	atp magazin
2019	Serangan siber & darknet - temu bual dengan Jean Pereira	Podcast "IT'S IN YOU"
2018	SEO-DAY: cara menggodam Chrome dan memintas SSL pada 2018	Host Europe
2018	Ceramah keselamatan dalam superpanel SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker dan pengasas SECBIZ dalam senarai penceramah	DSS IT SEC / Riga