Jean Pereira

งานวิจัยด้านความปลอดภัย · Offensive Security · Full-Stack Engineering

ผมวิจัยช่องโหว่ในระบบที่ซับซ้อน และพัฒนาซอฟต์แวร์ด้านความปลอดภัยรวมถึงผลิตภัณฑ์ของตนเองในด้านความปลอดภัยของเบราว์เซอร์ ระบบ embedded และอุตสาหกรรม ระบบอัตโนมัติ และ AI

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

โปรไฟล์

ผมพบช่องโหว่ด้านความปลอดภัยในจุดที่คนอื่นหยุดค้นหา และสร้างซอฟต์แวร์ที่ปลอดภัยเพื่อแก้ปัญหาที่ซับซ้อน

ผลงานของผมรวมถึงช่องโหว่ในผลิตภัณฑ์และเทคโนโลยีของ **Siemens**, **Apple**, **Google**, **Microsoft** และ **Nokia** รวมถึงโครงการต่าง ๆ ด้านเทคโนโลยีการแพทย์ ปัจจุบันผมมุ่งเน้นการวิจัยด้านความปลอดภัยและวิศวกรรมซอฟต์แวร์

ฉันยังเป็นผู้สร้าง **Veloce** อีกด้วย คุณสามารถติดต่อฉันผ่านแบบฟอร์มติดต่อ หรือทาง LinkedIn ได้โดยตรง

ไฮไลต์

ช่องโหว่ซีโร่เดย์สี่รายการของ **Siemens:** ยึดระบบเตือนภัยและอุปกรณ์ตรวจจับเพลิงไหม้จากระยะไกล

ผมยึดควบคุมระบบเตือนภัยและอุปกรณ์ตรวจจับเพลิงไหม้ของ Siemens ได้ทั้งหมดจากระยะไกล เอ็กซ์พลอยต์ของผมให้สิทธิ์ root ซึ่งเป็นสิทธิ์ระบบสูงสุด โดยไม่ต้องมีข้อมูลเข้าสู่ระบบ การคลิก หรือการโต้ตอบใดจากผู้เสียหาย

ผมพัฒนาเชนเอ็กซ์พลอยต์ที่รวมช่องโหว่ไม่เคยมีรายงานสี่รายการ และพิสูจน์การยึดควบคุมทั้งหมดได้จริง นี่คือการควบคุมเทคโนโลยีแจ้งเตือนที่สำคัญต่อความปลอดภัย

Siemens ยืนยันทั้งสี่รายการเป็น CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904 เอ็กซ์พลอยต์ได้รับคะแนน CVSS 10.0 ซึ่งหมายถึงความรุนแรงสูงสุดที่เป็นไปได้

ซีโร่เดย์ในโรงพยาบาล: แก้ไขหมู่เลือด ปิดสัญญาณเตือน **ECG** และอุปกรณ์ระบายอากาศได้จริง

ในการประเมินความปลอดภัย ผมพบ 22 ช่องโหว่ที่ยังไม่เคยมีรายงานในอุปกรณ์ของผู้ผลิตสิบสองราย และสาธิตการโจมตีด้วยเอ็กซ์พลอยต์จริง: ปิดสัญญาณเตือน ECG หยุดระบบระบายอากาศในห้องผ่าตัดปลอดเชื้อ และแก้ไขหมู่เลือดกับข้อมูลการแพ้ ผมยังพัฒนาการข้าม SOP/CORS เพื่อสาธิตการโจมตีระยะไกลต่ออุปกรณ์ภายในที่เข้าถึงจากอินเทอร์เน็ตโดยตรงไม่ได้

ผู้ผลิตที่ตรวจสอบรวมถึง ZEISS, MOXA, Zebra, Dedalus Labor และ Tetronik ตามรายงาน Golem ปี 2024 อุปกรณ์ดังกล่าวถูกใช้ในโรงพยาบาลและสถานพยาบาลอื่นอีกหลายพันแห่ง ผมประสานการเปิดเผยต่อผู้ผลิตและสนับสนุนการแก้ไข นักข่าวติดตามกระบวนการทั้งหมด ตั้งแต่แจ้งผู้ผลิตจนถึงการสนับสนุนการแก้ไขของผม

ช่องโหว่ในหน่วยงานรัฐกว่า **40** แห่ง **OBI, REWE** และสถาบัน **Fraunhofer**

ผมพบช่องโหว่ในเทศบาลและบริษัท 45 แห่ง และแจ้งผู้รับผิดชอบ ที่ OBI ช่องโหว่เว็บทำให้ยึดเซสชันผู้ใช้และอ่านข้อมูลจากระบบจัดการเนื้อหาภายในได้

เทศบาลหลายแห่งแก้ไขปัญหาแล้ว OBI ปิดเว็บไซต์ที่เกี่ยวข้องหลังเกิดข้อถกเถียงสาธารณะ Golem และ WirtschaftsWoche รายงานงานวิจัยและการตอบสนองของบริษัท

ประสบการณ์

มิ.ย. 2566 - ปัจจุบัน

CEO · CTO · CYTRES GmbH
ก่อตั้งและบริหารบริษัทโดยมุ่งเน้นการพัฒนาซอฟต์แวร์และการวิจัยความปลอดภัยไซเบอร์

ธ.ค. 2559 - ส.ค. 2562

ผู้สอนด้านความปลอดภัยไซเบอร์ · CIC (Cambridge Innovation Center) · Rotterdam, เนเธอร์แลนด์
จัดเวิร์กช็อปด้านความปลอดภัยไซเบอร์และการฝึกอบรมทางเทคนิค

ธ.ค. 2559 - ส.ค. 2562

ที่ปรึกษาความปลอดภัยอาวุโส · Base Cyber Security · Rotterdam, เนเธอร์แลนด์
ดูแลทีมเทคนิคและฝึกอบรมพนักงานใหม่ให้ถึงมาตรฐานทางเทคนิคที่กำหนด

2019

ผู้ก่อตั้ง · CEO · CTO · Secbiz IT Security GmbH
- ผู้ก่อตั้งและผู้นำด้านเทคนิคของบริษัทความปลอดภัยไซเบอร์
- วิจัยและให้คำปรึกษาด้านความปลอดภัยอุตสาหกรรม/OT และแอปพลิเคชัน
- สาธิตการโจมตี SCADA สดในงาน Hannover Messe 2019

Veloce

Veloce คือ JavaScript/TypeScript runtime ของผมสำหรับ agentic coding: เป็นแพลตฟอร์มเป้าหมายที่ coding agent สามารถสร้างแอปพลิเคชันที่สมบูรณ์ อ่านเข้าใจได้ ตรวจสอบได้ และรันได้ทันที โดยไม่ต้องประกอบ npm dependencies, frameworks, build tooling และ deployment glue ก่อน

runtime มีองค์ประกอบสำคัญมาให้ในตัว ได้แก่ sandbox และ permission model แบบจำกัด, HTTP server, SQLite และ PostgreSQL พร้อม ORM และ KV store, ความสามารถด้าน browser และ desktop และการ package เป็น native binary แบบ standalone งานคำนวณหนักสามารถย้ายจาก JavaScript/TypeScript ไปยัง native kernel ที่ใช้ Rust หรือ WebAssembly ได้ เป้าหมายคือซอฟต์แวร์ที่ agent สร้างได้อย่างเชื่อถือได้ คนยังอ่านเข้าใจได้ และระบบรันได้ด้วย moving parts ให้น้อยที่สุด

ความเชี่ยวชาญ

Embedded, OT และอุปกรณ์การแพทย์

วิจัยช่องโหว่ใน firmware และอุปกรณ์เชื่อมต่อ ได้แก่ ระบบแจ้งเหตุเพลิงไหม้ ตัวควบคุมอุตสาหกรรม (SCADA) อุปกรณ์โรงพยาบาล และอุปกรณ์การแพทย์

Exploit development

ตั้งแต่ข้อผิดพลาด memory corruption รายการเดียวไปจนถึง exploit chain แบบเต็มที่ให้ remote root access

ความปลอดภัยของ **browser** และ **web**

SOP/CORS bypass, เส้นทางโจมตีไปยังอุปกรณ์ในเครือข่ายภายใน, XSS และความปลอดภัยของแอปพลิเคชัน

Responsible disclosure

การรายงานและประสานงานกับผู้ผลิตและผู้ให้บริการ ตั้งแต่บริษัทขนาดใหญ่ถึงหน่วยงานเทศบาล รวมถึงช่วยสนับสนุนการแก้ไข

เครื่องมือของตนเอง

Tooling และ automation สำหรับการค้นหาช่องโหว่และ penetration testing รวมถึง workflow ที่ใช้ AI ช่วย ผู้สร้าง JavaScript/TypeScript runtime Veloce

งานวิจัย

ปี	งานวิจัย / ช่องโหว่	แหล่งอ้างอิง
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	รายการ CISA ที่ CIRCL
2013	Apple Motion - CVE-2013-6114 - ช่องโหว่ด้านความปลอดภัย	Apple
2014	Apple Web Server - งานวิจัยด้านความปลอดภัย, กุมภาพันธ์ 2557	Apple
2012	Nokia Hall of Fame - งานวิจัยด้านความปลอดภัย, ธันวาคม 2555	Nokia
2012	Android Browser DoS - CVE-2012-6301 - โมดูล Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	คลัง 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
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

สื่อ

ปี	บทความต้นฉบับ	สื่อ
2025	รายงานเกี่ยวกับการเปิดเผยช่องโหว่อย่างรับผิดชอบที่ Securitas / Marvelit	Security-Insider
2022	รายการวิทยุเกี่ยวกับความปลอดภัยไซเบอร์และการแฮ็กอย่างมีจริยธรรม	WDR
2024	เสวนาผู้เชี่ยวชาญ ÖAG: ความปลอดภัย 4.0 - ความปลอดภัยไซเบอร์และการป้องกันด้วย AI	medianet (ออสเตรีย)
2024	ช่องโหว่ด้านความปลอดภัยในโรงพยาบาล: ผู้ป่วยตกอยู่ในความเสี่ยง	Golem
2024	SOP/CORS ของเบราว์เซอร์และอุปกรณ์ในเครือข่ายภายใน	CYTRES Research
2024	ประกาศด้านความปลอดภัยต่อสาธารณะของ Jean Pereira พร้อมอัปเดตการแก้ไขที่มีการบันทึกไว้	Volksbank / Sparda Bank (Responsible Disclosure)
2023	เสวนาผู้เชี่ยวชาญกับรัฐมนตรีช่วย Tursky เรื่องดิจิทัล AI และความปลอดภัยไซเบอร์	KURIER (ออสเตรีย)
2023	เข้าร่วม ÖAG Super Tuesday ในฐานะผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์	LEADERSNET (ออสเตรีย)
2022	พอดแคสต์ #51: Ethical Hacker - งานวิจัยด้านความปลอดภัยและเส้นทางอาชีพ	IDG TechTalk / COMPUTERWOCHE
2022	ช่องโหว่ด้านความปลอดภัยไอทีของเมืองโคโลญ	Kölner Stadt-Anzeiger
2022	กรรมาธิการคุ้มครองข้อมูลสอบสวนกรณีช่องโหว่ความปลอดภัยที่มีผู้รายงานถูกเพิกเฉย	WirtschaftsWoche
2022	การเปิดเผยอย่างรับผิดชอบ / 45 องค์กร	Golem
2022	รายงานเกี่ยวกับ OBI และหน่วยงานภาครัฐ	connect professional
2020	คีย์โน้ตเรื่องความปลอดภัยของเบราว์เซอร์และแอปพลิเคชัน	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: แฮ็ก SCADA/ICS แบบสด	Hannover Messe / MittelstandsWiki
2019	สัมภาษณ์ "เราต้องการแฮ็กเกอร์มากกว่านี้"	atp magazin
2019	การโจมตีไซเบอร์และดาร์กเน็ต - สัมภาษณ์ Jean Pereira	Podcast "IT'S IN YOU"
2018	SEO-DAY: วิธีแฮ็ก Chrome และข้าม SSL ในปี 2018	Host Europe
2018	บรรยายด้านความปลอดภัยใน superpanel ของ SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker และผู้ก่อตั้ง SECBIZ อยู่ในรายชื่อวิทยากร	DSS IT SEC / Riga