Jean Pereira

Cercetare de securitate · Securitate ofensivă · Inginerie full-stack

Cercetez vulnerabilități în sisteme complexe și dezvolt software de securitate și produse proprii pentru securitatea browserelor, sisteme embedded și industriale, automatizare și AI.

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

Profil

Găsesc vulnerabilități de securitate acolo unde alții încetează să caute și dezvolt software sigur care rezolvă probleme complexe.

Activitatea mea include vulnerabilități în produse și tehnologii de la **Siemens**, **Apple**, **Google**, **Microsoft** și **Nokia**, precum și diverse proiecte în domeniul tehnologiei medicale. În prezent mă concentrez pe cercetarea în securitate și ingineria software.

Sunt și autorul **Veloce**. Mă poți contacta prin formularul de contact sau direct pe LinkedIn.

Repere

Patru zero-days la Siemens: sisteme de alarmă și detectoare de incendiu preluate de la distanță

Am preluat de la distanță controlul complet al sistemelor de alarmă și detectoarelor de incendiu Siemens. Exploitul meu mi-a oferit acces root, cele mai înalte privilegii de sistem, fără credențiale, clicuri sau alte acțiuni ale victimei.

Am dezvoltat un lanț de exploatare care combină patru vulnerabilități necunoscute și am demonstrat preluarea completă în practică. Era vorba despre controlul unei tehnologii de alarmare esențiale pentru siguranță.

Siemens a confirmat cele patru descoperiri, CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Exploitul a primit CVSS 10.0, gravitatea maximă posibilă.

Zero-days în spitale: grupe sanguine manipulate, alarme ECG și echipamente de ventilație ambientală oprite

Într-o analiză de securitate am descoperit 22 de vulnerabilități necunoscute în dispozitive de la doisprezece producători și am demonstrat atacurile cu exploituri funcționale: oprirea alarmelor ECG, întreruperea ventilației sălilor de operație sterile și manipularea grupelor sanguine și alergiilor. Am dezvoltat și ocoliri SOP/CORS pentru atacuri de la distanță asupra dispozitivelor interne inaccesibile direct din internet.

Producătorii investigați includ ZEISS, MOXA, Zebra, Dedalus Labor și Tetronik. Conform reportajului Golem din 2024, dispozitivele erau folosite în mii de alte spitale și unități medicale. Am coordonat divulgarea și am sprijinit remedierea. Jurnaliștii au urmărit întregul proces, de la notificarea producătorilor până la sprijinul meu pentru remediere.

Vulnerabilități la peste 40 de autorități, OBI, REWE și Institutul Fraunhofer

Am descoperit vulnerabilități la 45 de administrații municipale și companii și le-am raportat responsabililor. La OBI, o vulnerabilitate web permitea preluarea sesiunilor utilizatorilor și accesarea informațiilor din sistemul intern de gestionare a conținutului.

Multe administrații au remediat problemele. OBI a retras site-ul afectat după disputa publică. Golem și WirtschaftsWoche au documentat cercetarea și reacțiile companiilor.

Experiență

iun. 2023 - prezent

CEO · CTO · CYTRES GmbH
Am fondat și condus compania, cu accent pe dezvoltare software și cercetare în securitate cibernetică.

dec. 2016 - aug. 2019

Tutor de securitate cibernetică · CIC (Cambridge Innovation Center) · Rotterdam, Țările de Jos
Am susținut ateliere de securitate cibernetică și cursuri tehnice.

dec. 2016 - aug. 2019

Consilier senior de securitate · Base Cyber Security · Rotterdam, Țările de Jos
Am condus echipa tehnică și am instruit noii angajați până la nivelul tehnic necesar.

2019

Fondator · CEO · CTO · Secbiz IT Security GmbH

- Fondator și lider tehnic al unei companii de securitate cibernetică.
- Cercetare și consultanță în securitate industrială/OT și a aplicațiilor.
- Demonstrație SCADA live la Hannover Messe 2019.

Veloce

Veloce este runtime-ul meu JavaScript/TypeScript pentru agentic coding: o platformă țintă pe care agenții de programare pot crea aplicații complete, lizibile, auditabile și direct executabile, fără să asambleze mai întâi dependențe npm, framework-uri, tool-uri de build și glue de deployment.

Runtime-ul include direct componentele importante: sandbox și model de permisiuni restrictive, server HTTP, SQLite și PostgreSQL cu ORM și stocare KV, funcții pentru browser și desktop și împachetare într-un binar nativ autonom. Căile de calcul intensive pot fi mutate din JavaScript/TypeScript către kerneluri native bazate pe Rust sau WebAssembly. Scopul este software pe care agenții îl pot genera fiabil, oamenii îl pot înțelege în continuare, iar sistemele îl pot rula cu cât mai puține piese în mișcare.

Expertiză

Embedded, OT și tehnologie medicală

Cercetare de vulnerabilități în firmware și dispozitive conectate: sisteme de alarmă la incendiu, controlere industriale (SCADA), echipamente spitalicești și medicale.

Dezvoltare de exploituri

De la o singură vulnerabilitate de tip memory corruption la un lanț complet de exploituri cu acces root de la distanță.

Securitatea browserelor și web

Bypass-uri SOP/CORS, căi de atac către dispozitive din rețele interne, XSS și securitatea aplicațiilor.

Dezvăluire responsabilă

Raportare și coordonare cu producători și operatori, de la corporații mari la administrații municipale, inclusiv sprijin pentru remediere.

Instrumente proprii

Instrumente și automatizare pentru descoperirea vulnerabilităților și testarea penetrării, inclusiv workflow-uri asistate de AI. Autor al runtime-ului JavaScript/TypeScript Veloce.

Cercetare

An	Cercetare / vulnerabilitate	Sursă
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	înregistrare CISA la CIRCL
2013	Apple Motion - CVE-2013-6114 - vulnerabilitate	Apple
2014	Apple Web Server - cercetare de securitate, februarie 2014	Apple
2012	Nokia Hall of Fame - cercetare de securitate, decembrie 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - modul Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	arhiva 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

An	Cercetare / vulnerabilitate	Sursă
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

Presă

An	Articol original	Publicație
2025	Relatare despre responsible disclosure la Securitas / Marvelit	Security-Insider
2022	Intervenție radio despre securitate cibernetică și hacking etic	WDR
2024	Discuție ÖAG cu experți: Securitate 4.0 - securitate cibernetică și apărare cu IA	medianet (Austria)
2024	Vulnerabilități de securitate în spitale: pacienți în pericol	Golem
2024	SOP/CORS în browser și dispozitive din rețeaua internă	CYTRES Research
2024	Avertizare publică de securitate a lui Jean Pereira cu actualizare documentată privind remedierea	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Discuție cu secretarul de stat Tursky despre digitalizare, IA și securitate cibernetică	KURIER (Austria)
2023	Participare ca expert în securitate cibernetică la ÖAG Super Tuesday	LEADERSNET (Austria)
2022	Podcast #51: Ethical Hacker - cercetare de securitate și parcurs profesional	IDG TechTalk / COMPUTERWOCHE
2022	Vulnerabilitate de securitate IT la municipalitatea Köln	Kölner Stadt-Anzeiger
2022	Comisara pentru protecția datelor investighează o vulnerabilitate de securitate raportată și ignorată	WirtschaftsWoche
2022	Responsible disclosure / 45 de organizații	Golem
2022	Relatare despre OBI și autorități	connect professional
2020	Keynote despre securitatea browserelor și aplicațiilor	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: hacking SCADA/ICS în direct	Hannover Messe / MittelstandsWiki
2019	Interviu "Avem nevoie de mai mulți hackeri"	atp magazin
2019	Atacuri cibernetice și darknet - Jean Pereira în interviu	Podcast "IT'S IN YOU"
2018	SEO-DAY: cum să hackuiești Chrome și să ocolești SSL în 2018	Host Europe
2018	Prezentare de securitate în superpanelul SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker și fondatorul SECBIZ în lista vorbitorilor	DSS IT SEC / Riga