Jean Pereira

Recherche en sécurité · Sécurité offensive · Ingénierie full-stack

J'étudie les vulnérabilités de systèmes complexes et développe des logiciels de sécurité ainsi que mes propres produits dans les domaines de la sécurité des navigateurs, des systèmes embarqués et industriels, de l'automatisation et de l'IA.

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

Profil

Je trouve des failles de sécurité là où les autres cessent de chercher et je développe des logiciels sûrs qui résolvent des problèmes complexes.

Mes travaux comprennent des vulnérabilités dans des produits et technologies de **Siemens**, **Apple**, **Google**, **Microsoft** et **Nokia**, ainsi que divers projets dans le domaine des technologies médicales. Je me concentre actuellement sur la recherche en sécurité et l'ingénierie logicielle.

Je suis également l'auteur de **Veloce**. Tu peux me joindre via le formulaire de contact ou directement sur LinkedIn.

Points forts

Quatre zero-days chez Siemens: systèmes d'alarme et détecteurs d'incendie pris en main à distance

J'ai pris le contrôle complet à distance de systèmes d'alarme et de détecteurs d'incendie Siemens. Mon exploit m'a donné les droits root, les privilèges système les plus élevés, sans identifiants, clic ni autre intervention de la victime.

J'ai développé une chaîne d'exploitation combinant quatre vulnérabilités inconnues et démontré cette prise de contrôle en pratique. Il s'agissait du contrôle d'une technologie d'alarme essentielle à la sécurité.

Siemens a confirmé les quatre découvertes, CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. L'exploit a reçu CVSS 10.0, la criticité maximale possible.

Zero-days dans les hôpitaux : groupes sanguins modifiés, alarmes ECG et équipements de ventilation désactivés

Lors d'un audit, j'ai découvert 22 vulnérabilités jusque-là inconnues dans les appareils de douze fabricants et démontré les attaques avec des exploits fonctionnels : désactivation d'alarmes ECG, interruption de la ventilation de blocs opératoires stériles et manipulation des groupes sanguins et des allergies. Mes contournements SOP/CORS ont aussi démontré des attaques à distance contre des appareils internes non accessibles directement depuis Internet.

Les fabricants étudiés incluent ZEISS, MOXA, Zebra, Dedalus Labor et Tetronik. Selon le reportage de Golem de 2024, ces appareils équipaient des milliers d'autres hôpitaux et établissements médicaux. J'ai coordonné la divulgation et accompagné les corrections. Des journalistes ont suivi tout le processus, du signalement aux fabricants à mon accompagnement des corrections.

Des failles dans plus de 40 administrations, chez OBI, REWE et à l'institut Fraunhofer

J'ai découvert des vulnérabilités dans 45 collectivités et entreprises et les ai signalées aux responsables. Chez OBI, une faille web permettait le détournement de sessions et l'accès aux informations du système interne de gestion de contenu.

De nombreuses collectivités ont corrigé les failles. OBI a retiré le site concerné après la controverse publique. Golem et WirtschaftsWoche ont documenté la recherche et les réactions des entreprises.

Expérience

juin 2023 - aujourd'hui

CEO · CTO · CYTRES GmbH
Création et direction de l'entreprise, axées sur le développement logiciel et la recherche en cybersécurité.

déc. 2016 - août 2019

Tuteur en cybersécurité · CIC (Cambridge Innovation Center) · Rotterdam, Pays-Bas
Animation d'ateliers de cybersécurité et de formations techniques.

déc. 2016 - août 2019

Conseiller senior en sécurité · Base Cyber Security · Rotterdam, Pays-Bas
Direction de l'équipe technique ainsi qu'intégration et formation des nouveaux collaborateurs jusqu'au niveau technique requis.

2019

Fondateur · CEO · CTO · Secbiz IT Security GmbH
- Fondateur et responsable technique d'une entreprise de cybersécurité.
- Recherche et conseil en sécurité industrielle/OT et applicative.
- Démonstration d'attaque sur système SCADA au salon de Hanovre en 2019.

Veloce

Veloce est mon runtime JavaScript/TypeScript conçu pour le développement agentique : une plateforme cible sur laquelle des agents de code peuvent produire des applications complètes, lisibles, auditables et directement exécutables, sans devoir assembler au préalable des dépendances npm, des frameworks, une chaîne de build et tout le glue de déploiement.

Le runtime intègre directement les briques essentielles : sandbox et modèle de permissions restrictifs, serveur HTTP, SQLite et PostgreSQL avec ORM et stockage KV, fonctions navigateur et desktop, ainsi que le packaging en binaire natif autonome. Les chemins de calcul intensifs peuvent être déportés depuis JavaScript/TypeScript vers des kernels natifs basés sur Rust ou WebAssembly. L'objectif est un logiciel que les agents peuvent générer de façon fiable, que les humains peuvent toujours comprendre et qui s'exécute avec le moins de composants mobiles possible.

Compétences

Systèmes embarqués, OT et dispositifs médicaux

Recherche de vulnérabilités dans le firmware et les appareils connectés : systèmes d'alarme incendie, contrôleurs industriels (SCADA), équipements hospitaliers et médicaux.

Développement d'exploits

D'une vulnérabilité de corruption mémoire isolée à une chaîne d'exploitation complète avec accès root à distance.

Sécurité des navigateurs et du web

Contournements SOP/CORS, chemins d'attaque vers des appareils du réseau interne, XSS et sécurité applicative.

Divulgation responsable

Signalement et coordination avec les fabricants et exploitants, des grands groupes aux administrations municipales, avec accompagnement de la remédiation.

Outils propres

Outils et automatisation pour la recherche de vulnérabilités et les tests d'intrusion, y compris des workflows assistés par l'IA. Auteur de la runtime JavaScript/TypeScript Veloce.

Recherche

Année	Recherche / vulnérabilité	Source
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	entrée CISA chez CIRCL
2013	Apple Motion - CVE-2013-6114 - vulnérabilité	Apple
2014	Apple Web Server - recherche en sécurité, février 2014	Apple
2012	Nokia Hall of Fame - recherche en sécurité, décembre 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - module Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	archive Bugtraq
2012	PhpTax - CVE-2012-10037 - Remote Command Injection	OpenCVE

Année	Recherche / vulnérabilité	Source
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

Presse

Année	Publication originale	Média
2025	Couverture de la divulgation responsable chez Securitas / Marvelit	Security-Insider
2022	Émission radio sur la cybersécurité et le hacking éthique	WDR
2024	Table ronde d'experts de l'ÖAG : Sécurité 4.0 - cybersécurité et défense par l'IA	medianet (Autriche)
2024	Failles de sécurité dans les hôpitaux : des patients en danger	Golem
2024	SOP/CORS du navigateur et appareils du réseau interne	CYTRES Research
2024	Alerte de sécurité publique de Jean Pereira avec mise à jour documentée de la correction	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Table ronde avec le secrétaire d'État Tursky sur la numérisation, l'IA et la cybersécurité	KURIER (Autriche)
2023	Participation en tant qu'expert en cybersécurité au Super Tuesday de l'ÖAG	LEADERSNET (Autriche)
2022	Podcast n° 51 : Ethical Hacker - recherche en sécurité et parcours professionnel	IDG TechTalk / COMPUTERWOCHE
2022	Faille de sécurité informatique à la ville de Cologne	Kölner Stadt-Anzeiger
2022	La commissaire à la protection des données enquête après le signalement ignoré d'une faille de sécurité	WirtschaftsWoche
2022	Divulgation responsable / 45 organisations	Golem
2022	Reportage sur OBI et les administrations publiques	connect professional
2020	Keynote sur la sécurité des navigateurs et des applications	OMT - Online Marketing Konferenz
2019	Industrial Security Forum : hacking SCADA/ICS en direct	Hannover Messe / MittelstandsWiki
2019	Interview « Nous avons besoin de plus de hackers »	atp magazin
2019	Cyberattaques & darknet - Jean Pereira en interview	Podcast "IT'S IN YOU"
2018	SEO-DAY : comment pirater Chrome et contourner SSL en 2018	Host Europe
2018	Conférence sur la sécurité dans le superpanel du SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference : Ethical Hacker et fondateur de SECBIZ parmi les intervenants	DSS IT SEC / Riga