Jean Pereira

Ricerca sulla sicurezza · Offensive security · Ingegneria full-stack

Studio vulnerabilità in sistemi complessi e sviluppo software di sicurezza e prodotti indipendenti nei settori della sicurezza dei browser, dei sistemi embedded e industriali, dell'automazione e dell'IA.

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

Profilo

Trovo vulnerabilità di sicurezza dove altri smettono di cercare e sviluppo software sicuro che risolve problemi complessi.

Il mio lavoro comprende vulnerabilità in prodotti e tecnologie di **Siemens**, **Apple**, **Google**, **Microsoft** e **Nokia**, oltre a vari progetti nel settore delle tecnologie mediche. Attualmente mi concentro sulla ricerca in sicurezza e sull'ingegneria del software.

Sono anche l'autore di **Veloce**. Puoi contattarmi tramite il modulo di contatto o direttamente su LinkedIn.

In evidenza

Quattro zero-day in Siemens: sistemi di allarme e rilevatori d'incendio controllati da remoto

Ho assunto da remoto il controllo completo di sistemi di allarme e rilevatori d'incendio Siemens. Il mio exploit mi ha dato accesso root, i massimi privilegi di sistema, senza credenziali, clic o altre azioni della vittima.

Ho sviluppato una catena di exploit combinando quattro vulnerabilità sconosciute e dimostrato concretamente la completa acquisizione del controllo. Si trattava di tecnologia di allarme essenziale per la sicurezza.

Siemens ha confermato i quattro risultati, da CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. L'exploit ha ricevuto CVSS 10.0, la massima criticità possibile.

Zero-day negli ospedali: gruppi sanguigni manipolati, allarmi ECG e dispositivi di ventilazione ambientale disattivati

Durante una verifica ho scoperto 22 vulnerabilità sconosciute in dispositivi di dodici produttori e dimostrato gli attacchi con exploit funzionanti: disattivazione degli allarmi ECG, interruzione della ventilazione delle sale operatorie sterili e manipolazione di gruppi sanguigni e allergie. Ho inoltre sviluppato bypass SOP/CORS per dimostrare attacchi remoti contro dispositivi interni non direttamente raggiungibili da Internet.

Tra i produttori analizzati figurano ZEISS, MOXA, Zebra, Dedalus Labor e Tetronik. Secondo il reportage Golem del 2024, i dispositivi interessati erano utilizzati in migliaia di altri ospedali e strutture mediche. Ho coordinato la divulgazione e supportato le correzioni. I giornalisti hanno seguito l'intero processo, dalla segnalazione ai produttori al mio supporto per le correzioni.

Vulnerabilità in oltre 40 enti pubblici, OBI, REWE e nell'Istituto Fraunhofer

Ho scoperto vulnerabilità in 45 amministrazioni comunali e aziende e le ho segnalate ai responsabili. In OBI, una vulnerabilità web consentiva il dirottamento delle sessioni e l'accesso a informazioni del sistema interno di gestione dei contenuti.

Molte amministrazioni hanno corretto le falle. OBI ha ritirato il sito coinvolto dopo la controversia pubblica. Golem e WirtschaftsWoche hanno documentato la ricerca e le reazioni delle aziende.

Esperienza

giu 2023 - oggi

CEO · CTO · CYTRES GmbH
Ho fondato e diretto l'azienda con particolare attenzione allo sviluppo software e alla ricerca in cybersecurity.

dic 2016 - ago 2019

Tutor di cybersecurity · CIC (Cambridge Innovation Center) · Rotterdam, Paesi Bassi
Ho tenuto workshop di cybersecurity e corsi di formazione tecnica.

dic 2016 - ago 2019

Senior Security Advisor · Base Cyber Security · Rotterdam, Paesi Bassi
Ho guidato il team tecnico e formato i nuovi dipendenti fino al raggiungimento dello standard tecnico richiesto.

2019

Fondatore · CEO · CTO · Secbiz IT Security GmbH

- Fondatore e responsabile tecnico di un'azienda di sicurezza informatica.
- Ricerca e consulenza per sicurezza industriale/OT e applicativa.
- Dimostrazione dal vivo su SCADA alla Hannover Messe 2019.

Veloce

Veloce è il mio runtime JavaScript/TypeScript per l'agentic coding: una piattaforma di destinazione su cui gli agenti di coding possono creare applicazioni complete, leggibili, verificabili e immediatamente eseguibili, senza dover prima assemblare dipendenze npm, framework, tool di build e glue di deployment.

Il runtime include direttamente i componenti essenziali: sandbox e modello di permessi restrittivi, server HTTP, SQLite e PostgreSQL con ORM e KV store, funzionalità browser e desktop e packaging in un singolo binario nativo autonomo. I percorsi di calcolo intensivo possono essere spostati da JavaScript/TypeScript a kernel nativi basati su Rust o a WebAssembly. L'obiettivo è software che gli agenti possano generare in modo affidabile, che le persone possano ancora comprendere e che i sistemi possano eseguire con il minor numero possibile di parti mobili.

Competenze

Sistemi embedded, OT e dispositivi medici

Ricerca di vulnerabilità in firmware e dispositivi connessi: sistemi antincendio, controllori industriali (SCADA), apparecchiature ospedaliere e medicali.

Sviluppo di exploit

Da una singola vulnerabilità di memory corruption a una exploit chain completa con accesso root remoto.

Sicurezza browser e web

Bypass SOP/CORS, percorsi di attacco verso dispositivi nelle reti interne, XSS e sicurezza applicativa.

Responsible disclosure

Segnalazione e coordinamento con produttori e operatori, dalle grandi aziende alle amministrazioni comunali, compreso il supporto alla correzione.

Strumenti propri

Tooling e automazione per la ricerca di vulnerabilità e il penetration testing, inclusi workflow assistiti da AI. Autore della runtime JavaScript/TypeScript Veloce.

Ricerca

Anno	Ricerca / vulnerabilità	Fonte
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	voce CISA su CIRCL
2013	Apple Motion - CVE-2013-6114 - vulnerabilità	Apple
2014	Apple Web Server - ricerca sulla sicurezza, febbraio 2014	Apple
2012	Nokia Hall of Fame - ricerca sulla sicurezza, dicembre 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - modulo Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	archivio 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

Anno	Ricerca / vulnerabilità	Fonte
2012	plow .plowrc - Buffer Overflow - BID 54290	Bugtraq
2012	Internet Explorer - XSS Filter Bypass - Exploit-DB 22100	VulDB

Stampa

Anno	Articolo originale	Testata
2025	Copertura sulla responsible disclosure presso Securitas / Marvelit	Security-Insider
2022	Servizio radiofonico su cybersecurity ed ethical hacking	WDR
2024	Incontro di esperti ÖAG: Sicurezza 4.0 - cybersecurity e difesa con l'IA	medianet (Austria)
2024	Vulnerabilità di sicurezza negli ospedali: pazienti a rischio	Golem
2024	SOP/CORS del browser e dispositivi della rete interna	CYTRES Research
2024	Segnalazione pubblica di sicurezza di Jean Pereira con aggiornamento documentato sulla correzione	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Incontro con il segretario di Stato Tursky su digitalizzazione, IA e cybersecurity	KURIER (Austria)
2023	Partecipazione come esperto di cybersecurity all'ÖAG Super Tuesday	LEADERSNET (Austria)
2022	Podcast #51: Ethical Hacker - ricerca sulla sicurezza e percorso professionale	IDG TechTalk / COMPUTERWOCHE
2022	Vulnerabilità di sicurezza informatica presso la città di Colonia	Kölner Stadt-Anzeiger
2022	La garante per la protezione dei dati indaga su una vulnerabilità di sicurezza segnalata e ignorata	WirtschaftsWoche
2022	Responsible disclosure / 45 organizzazioni	Golem
2022	Articolo su OBI e le autorità pubbliche	connect professional
2020	Keynote sulla sicurezza di browser e applicazioni	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: hacking SCADA/ICS dal vivo	Hannover Messe / MittelstandsWiki
2019	Intervista «Abbiamo bisogno di più hacker»	atp magazin
2019	Cyberattacchi e darknet - Jean Pereira in intervista	Podcast "IT'S IN YOU"
2018	SEO-DAY: come hackerare Chrome e aggirare SSL nel 2018	Host Europe
2018	Intervento sulla sicurezza nel superpanel del SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker e fondatore di SECBIZ tra gli speaker	DSS IT SEC / Riga