Jean Pereira

Säkerhetsforskning · Offensiv säkerhet · Fullstackutveckling

Jag forskar om sårbarheter i komplexa system och utvecklar säkerhetsprogramvara och egna produkter inom webbläsarsäkerhet, inbyggda och industriella system, automatisering och AI.

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

Profil

Jag hittar säkerhetsbrister där andra slutar leta och bygger säker programvara som löser komplexa problem.

Mitt arbete omfattar sårbarheter i produkter och teknik från **Siemens**, **Apple**, **Google**, **Microsoft** och **Nokia**, samt olika projekt inom medicinteknik. Mitt fokus ligger för närvarande på säkerhetsforskning och mjukvaruutveckling.

Jag är också skaparen av **Veloce**. Du når mig via kontaktformuläret eller direkt på LinkedIn.

Höjdpunkter

Fyra zero-days hos Siemens: larmsystem och branddetektorer övertagna på distans

Jag tog full kontroll på distans över larmsystem och branddetektorer från Siemens. Min exploit gav rootåtkomst, de högsta systembehörigheterna, utan inloggningsuppgifter, klick eller annan medverkan från offret.

Jag utvecklade en exploitkedja med fyra okända sårbarheter och demonstrerade det fullständiga övertagandet i praktiken. Det handlade om kontroll över säkerhetskritisk larmteknik.

Siemens bekräftade de fyra fynden som CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Exploiten fick betyget CVSS 10.0, högsta möjliga allvarlighetsgrad.

Zero-days på sjukhus: blodgrupper manipulerade, EKG-larm och ventilationsaggregat avstängda

Vid en säkerhetsgranskning upptäckte jag 22 tidigare okända sårbarheter i enheter från tolv tillverkare och demonstrerade angreppen med fungerande exploits: avstängning av EKG-larm, avbrott i ventilationen i sterila operationssalar och manipulation av blodgrupper och allergiuppgifter. Jag utvecklade även SOP/CORS-bypass för fjärrangrepp mot interna enheter som inte var direkt åtkomliga från internet.

Granskade tillverkare omfattar ZEISS, MOXA, Zebra, Dedalus Labor och Tetronik. Enligt Golems reportage 2024 användes enheterna på tusentals andra sjukhus och vårdinrättningar. Jag samordnade rapporteringen och stödde åtgärderna. Journalister följde hela processen, från rapportering till tillverkarna till mitt stöd vid åtgärderna.

Sårbarheter hos över 40 myndigheter, OBI, REWE och Fraunhoferinstitutet

Jag upptäckte sårbarheter hos 45 kommuner och företag och rapporterade dem till ansvariga team. Hos OBI möjliggjorde en webbsårbarhet kapning av användarsessioner och åtkomst till information i det interna publiceringssystemet.

Många kommuner åtgärdade bristerna. OBI tog den berörda webbplatsen offline efter den offentliga tvisten. Golem och WirtschaftsWoche dokumenterade forskningen och företagens reaktioner.

Erfarenhet

juni 2023 - nu

CEO · CTO · CYTRES GmbH
Grundade och ledde företaget med fokus på mjukvaruutveckling och cybersäkerhetsforskning.

dec. 2016 - aug. 2019

Handledare i cybersäkerhet · CIC (Cambridge Innovation Center) · Rotterdam, Nederländerna
Genomförde workshops i cybersäkerhet och tekniska utbildningar.

dec. 2016 - aug. 2019

Senior säkerhetsrådgivare · Base Cyber Security · Rotterdam, Nederländerna
Ledde det tekniska teamet och introducerade och utbildade nya medarbetare till den tekniska nivå som krävdes.

2019

Grundare · CEO · CTO · Secbiz IT Security GmbH

- Grundare och teknisk ledare för ett säkerhetsföretag.
- Forskning och rådgivning inom industriell/OT- och applikationssäkerhet.
- Livevisning av SCADA-hackning på Hannover Messe 2019.

Veloce

Veloce är min JavaScript/TypeScript-runtime för agentic coding: en målplattform där kodagenter kan skapa kompletta applikationer som är läsbara, granskningsbara och direkt körbara utan att först sätta ihop npm-beroenden, ramverk, byggverktyg och deployment-glue.

Runtime-miljön har de viktiga byggstenarna inbyggda: en restriktiv sandbox och behörighetsmodell, HTTP-server, SQLite och PostgreSQL med ORM och KV-lagring, browser- och desktopfunktioner samt paketering till en fristående native binary. Beräkningsintensiva delar kan flyttas från JavaScript/TypeScript till Rust-baserade native kernels eller WebAssembly. Målet är programvara som agenter kan generera pålitligt, människor fortfarande kan förstå och system kan köra med så få rörliga delar som möjligt.

Expertis

Inbyggda system, OT och medicinteknik

Sårbarhetsforskning i firmware och uppkopplade enheter: brandlarmsystem, industriella styrsystem (SCADA), sjukhus- och medicinteknisk utrustning.

Exploitutveckling

Från en enskild memory-corruption-sårbarhet till en fullständig exploitkedja med rootåtkomst på distans.

Webbläsar- och webbsäkerhet

SOP/CORS-bypasser, attackvägar till enheter i interna nätverk, XSS och applikationssäkerhet.

Ansvarsfull rapportering

Rapportering och samordning med tillverkare och operatörer, från stora företag till kommunala myndigheter, inklusive stöd vid åtgärd.

Egna verktyg

Verktyg och automatisering för sårbarhetsidentifiering och penetrationstestning, inklusive AI-assisterade arbetsflöden. Skapare av JavaScript/TypeScript-runtimen Veloce.

Forskning

År	Forskning / sårbarhet	Källa
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	CISA-post hos CIRCL
2013	Apple Motion - CVE-2013-6114 - sårbarhet	Apple
2014	Apple Web Server - säkerhetsforskning, februari 2014	Apple
2012	Nokia Hall of Fame - säkerhetsforskning, december 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit-modul	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq-arkiv
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

Press

År	Originalartikel	Medium
2025	Rapportering om responsible disclosure hos Securitas / Marvelit	Security-Insider
2022	Radioinslag om cybersäkerhet och etisk hackning	WDR
2024	ÖAG-expertsamtal: Säkerhet 4.0 - cybersäkerhet och AI-baserat försvar	medianet (Österrike)
2024	Säkerhetsbrister på sjukhus: patienter i fara	Golem
2024	Webbläsarens SOP/CORS och enheter i interna nätverk	CYTRES Research
2024	Offentlig säkerhetsrapport från Jean Pereira med dokumenterad uppdatering om åtgärden	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Expertsamtal med statssekreterare Tursky om digitalisering, AI och cybersäkerhet	KURIER (Österrike)
2023	Deltog som cybersäkerhetsexpert på ÖAG Super Tuesday	LEADERSNET (Österrike)
2022	Podcast #51: Ethical Hacker - säkerhetsforskning och karriärväg	IDG TechTalk / COMPUTERWOCHE
2022	IT-säkerhetsbrist hos staden Köln	Kölner Stadt-Anzeiger
2022	Dataskyddskommissionären utreder en rapporterad säkerhetsbrist som ignorerats	WirtschaftsWoche
2022	Responsible disclosure / 45 organisationer	Golem
2022	Rapport om OBI och myndigheter	connect professional
2020	Keynote om webbläsar- och applikationssäkerhet	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: livehackning av SCADA/ICS	Hannover Messe / MittelstandsWiki
2019	Intervju "Vi behöver fler hackers"	atp magazin
2019	Cyberattacker & darknet - intervju med Jean Pereira	Podcast "IT'S IN YOU"
2018	SEO-DAY: så hackar man Chrome och kringgår SSL 2018	Host Europe
2018	Säkerhetsföredrag i superpanelen på SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker och SECBIZ-grundare bland talarna	DSS IT SEC / Riga