Jean Pereira

Sikkerhetsforskning · Offensiv sikkerhet · Fullstackutvikling

Jeg undersøker sårbarheter i komplekse systemer og utvikler sikkerhetsprogramvare og egne produkter innen nettlesersikkerhet, innebygde og industrielle systemer, automatisering og KI.

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

Profil

Jeg finner sikkerhetshull der andre slutter å lete, og bygger sikker programvare som løser komplekse problemer.

Arbeidet mitt omfatter sårbarheter i produkter og teknologier fra **Siemens**, **Apple**, **Google**, **Microsoft** og **Nokia**, samt ulike prosjekter innen medisinsk teknologi. Mitt fokus er for tiden på sikkerhetsforskning og programvareutvikling.

Jeg er også utvikleren bak **Veloce**. Du kan nå meg via kontaktskjemaet eller direkte på LinkedIn.

Høydepunkter

Fire zero-days hos Siemens: alarmsystemer og branndetektorer overtatt på avstand

Jeg overtok på avstand full kontroll over alarmsystemer og branndetektorer fra Siemens. Min exploit ga root-tilgang, de høyeste systemrettighetene, uten innloggingsdata, klikk eller annen medvirkning fra offeret.

Jeg utviklet en exploitkjede med fire ukjente sårbarheter og demonstrerte den fullstendige overtakelsen i praksis. Det handlet om kontroll over sikkerhetskritisk alarmteknikk.

Siemens bekreftet de fire funnene som CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Exploiten fikk vurderingen CVSS 10.0, den høyest mulige alvorlighetsgraden.

Zero-days på sykehus: blodgrupper manipulert, EKG-alarmer og ventilasjonsanlegg slått av

Under en sikkerhetsanalyse oppdaget jeg 22 tidligere ukjente sårbarheter i enheter fra tolv produsenter og demonstrerte angrepene med fungerende exploits: deaktivering av EKG-alarmer, avbrudd i ventilasjonen på sterile operasjonsstuer og manipulering av blodgrupper og allergiopplysninger. Jeg utviklet også SOP/CORS-omgåelser for fjernangrep mot interne enheter uten direkte internettilgang.

Undersøkte produsenter omfatter ZEISS, MOXA, Zebra, Dedalus Labor og Tetronik. Ifølge Golems reportasje fra 2024 var enhetene i bruk på tusenvis av andre sykehus og medisinske institusjoner. Jeg koordinerte varslingen og støttet utbedringen. Journalister fulgte hele prosessen, fra varsling av produsentene til min støtte til utbedringen.

Sårbarheter hos over 40 myndigheter, OBI, REWE og Fraunhofer-instituttet

Jeg avdekket sårbarheter hos 45 kommuner og bedrifter og rapporterte dem til de ansvarlige. Hos OBI muliggjorde en nettsårbarhet overtakelse av brukerøkter og tilgang til informasjon i det interne publiseringssystemet.

Mange kommuner rettet feilene. OBI tok det berørte nettstedet offline etter den offentlige striden. Golem og WirtschaftsWoche dokumenterte forskningen og bedriftenes reaksjoner.

Erfaring

juni 2023 - nå

CEO · CTO · CYTRES GmbH
Grunnla og ledet selskapet med fokus på programvareutvikling og cybersikkerhetsforskning.

des. 2016 - aug. 2019

Veileder i cybersikkerhet · CIC (Cambridge Innovation Center) · Rotterdam, Nederland
Gjennomførte workshops i cybersikkerhet og tekniske kurs.

des. 2016 - aug. 2019

Senior sikkerhetsrådgiver · Base Cyber Security · Rotterdam, Nederland
Ledet det tekniske teamet og lærte opp nye medarbeidere til nødvendig teknisk nivå.

2019

Grunnlegger · CEO · CTO · Secbiz IT Security GmbH

- Grunnlegger og teknisk leder av et sikkerhetsselskap.
- Forskning og rådgivning om industriell/OT- og applikasjonssikkerhet.
- Live SCADA-hacking på Hannover Messe 2019.

Veloce

Veloce er min JavaScript/TypeScript-runtime for agentic coding: en målplattform der kodeagenter kan lage komplette applikasjoner som er lesbare, etterprøvbare og direkte kjørbare uten først å sette sammen npm-avhengigheter, rammeverk, byggeverktøy og deployment-glue.

Runtime-miljøet har de viktige byggesteinene innebygd: en restriktiv sandbox og tillatelsesmodell, HTTP-server, SQLite og PostgreSQL med ORM og KV-lagring, nettleser- og desktopfunksjoner samt pakking til én selvstendig native binary. Beregningstunge deler kan flyttes fra JavaScript/TypeScript til Rust-baserte native kernels eller WebAssembly. Målet er programvare som agenter kan generere pålitelig, mennesker fortsatt kan forstå og systemer kan kjøre med så få bevegelige deler som mulig.

Kompetanse

Innebygde systemer, OT og medisinsk teknologi

Sårbarhetsforskning i firmware og tilkoblede enheter: brannalarmsystemer, industrielle styringer (SCADA), sykehus- og medisinsk utstyr.

Exploit-utvikling

Fra én memory-corruption-feil til en komplett exploit-kjede med ekstern root-tilgang.

Nettleser- og websikkerhet

SOP/CORS-bypasser, angrepsveier til enheter i interne nettverk, XSS og applikasjonssikkerhet.

Ansvarlig disclosure

Rapportering og koordinering med produsenter og operatører, fra store selskaper til kommunale myndigheter, inkludert støtte ved utbedring.

Egne verktøy

Verktøy og automatisering for sårbarhetsfunn og penetrasjonstesting, inkludert KI-assisterte arbeidsflyter. Utvikleren bak JavaScript/TypeScript-runtimen Veloce.

Forskning

År	Forskning / sårbarhet	Kilde
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-oppføring hos CIRCL
2013	Apple Motion - CVE-2013-6114 - sårbarhet	Apple
2014	Apple Web Server - sikkerhetsforskning, februar 2014	Apple
2012	Nokia Hall of Fame - sikkerhetsforskning, desember 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

Presse

År	Originalartikkel	Medium
2025	Dekning av responsible disclosure hos Securitas / Marvelit	Security-Insider
2022	Radioinnslag om cybersikkerhet og etisk hacking	WDR
2024	ÖAG-ekspertsamtale: Sikkerhet 4.0 - cybersikkerhet og AI-basert forsvar	medianet (Østerrike)
2024	Sikkerhetssårbarheter på sykehus: pasienter i fare	Golem
2024	Nettleser-SOP/CORS og enheter i interne nettverk	CYTRES Research
2024	Offentlig sikkerhetsmelding fra Jean Pereira med dokumentert oppdatering om utbedringen	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Ekspertsamtale med statssekretær Tursky om digitalisering, AI og cybersikkerhet	KURIER (Østerrike)
2023	Deltok som cybersikkerhetsekspert på ÖAG Super Tuesday	LEADERSNET (Østerrike)
2022	Podcast #51: Ethical Hacker - sikkerhetsforskning og karrierevei	IDG TechTalk / COMPUTERWOCHE
2022	IT-sikkerhetssårbarhet hos byen Köln	Kölner Stadt-Anzeiger
2022	Personvernkommissæren undersøker en rapportert sikkerhetssårbarhet som ble ignorert	WirtschaftsWoche
2022	Responsible disclosure / 45 organisasjoner	Golem
2022	Rapport om OBI og offentlige myndigheter	connect professional
2020	Keynote om nettleser- og applikasjonssikkerhet	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: live SCADA/ICS-hacking	Hannover Messe / MittelstandsWiki
2019	Intervju «Vi trenger flere hackere»	atp magazin
2019	Cyberangrep & darknet - intervju med Jean Pereira	Podcast "IT'S IN YOU"
2018	SEO-DAY: slik hacker du Chrome og omgår SSL i 2018	Host Europe
2018	Sikkerhetsforedrag i superpanelet på SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker og SECBIZ-grunnlegger blant foredragsholderne	DSS IT SEC / Riga