# Jean Pereira

Securityonderzoek · Offensive security · Full-stack engineering

Ik onderzoek kwetsbaarheden in complexe systemen en ontwikkel beveiligingssoftware en eigen producten op het gebied van browserbeveiliging, embedded en industriële systemen, automatisering en AI.

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

## Profiel

Ik vind beveiligingslekken waar anderen stoppen met zoeken en bouw veilige software die complexe problemen oplost.

Mijn werk omvat kwetsbaarheden in producten en technologieën van **Siemens**, **Apple**, **Google**, **Microsoft** en **Nokia**, evenals diverse projecten binnen de medische technologie. Mijn focus ligt momenteel op security research en software engineering.

Daarnaast ben ik de auteur van **Veloce**. Je kunt me bereiken via het contactformulier of rechtstreeks op LinkedIn.

## Hoogtepunten

### Vier zero-days bij Siemens: alarmsystemen en brandmelders op afstand overgenomen

Ik nam op afstand de volledige controle over alarmsystemen en brandmelders van Siemens. Mijn exploit gaf mij roottoegang, de hoogste systeemrechten, zonder inloggegevens, klikken of andere medewerking van het slachtoffer.

Ik ontwikkelde een exploitketen van vier onbekende kwetsbaarheden en demonstreerde de volledige overname in de praktijk. Het ging om controle over alarmtechniek die cruciaal is voor de veiligheid.

Siemens bevestigde de vier bevindingen als CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. De exploit kreeg CVSS 10.0, de maximaal mogelijke ernst.

### Zero-days in ziekenhuizen: bloedgroepen gemanipuleerd, ECG-alarmen en ventilatieapparaten uitgeschakeld

Tijdens een beveiligingsonderzoek ontdekte ik 22 onbekende kwetsbaarheden in apparaten van twaalf fabrikanten en demonstreerde ik aanvallen met werkende exploits: ECG-alarmen uitschakelen, ventilatie van steriele operatiekamers onderbreken en bloedgroepen en allergiegegevens manipuleren. Met zelf ontwikkelde SOP/CORS-bypasses demonstreerde ik ook aanvallen op interne apparaten die niet rechtstreeks via internet bereikbaar waren.

Onderzochte fabrikanten zijn onder meer ZEISS, MOXA, Zebra, Dedalus Labor en Tetronik. Volgens Golems reportage uit 2024 werden de getroffen apparaten in duizenden andere ziekenhuizen en medische instellingen gebruikt. Ik coördineerde de melding en ondersteunde het herstel. Journalisten volgden het hele proces, van de melding aan fabrikanten tot mijn ondersteuning bij het verhelpen van de kwetsbaarheden.

### Kwetsbaarheden bij meer dan 40 overheidsinstanties, OBI, REWE en het Fraunhofer-instituut

Ik ontdekte kwetsbaarheden bij 45 gemeenten en bedrijven en meldde ze aan de verantwoordelijke teams. Bij OBI maakte een webkwetsbaarheid het overnemen van gebruikerssessies en uitlezen van informatie uit het interne contentmanagementsysteem mogelijk.

Veel gemeenten verhielpen de gemelde fouten. OBI haalde de getroffen website offline na de publieke discussie. Golem en WirtschaftsWoche documenteerden het onderzoek en de reacties van de bedrijven.

## Ervaring

jun 2023 - heden

**CEO · CTO** · CYTRES GmbH
Het bedrijf opgericht en geleid met de nadruk op softwareontwikkeling en cybersecurityonderzoek.

dec 2016 - aug 2019

**Tutor cybersecurity** · CIC (Cambridge Innovation Center) · Rotterdam, Nederland
Cybersecurityworkshops en technische trainingen verzorgd.

dec 2016 - aug 2019

**Senior beveiligingsadviseur** · Base Cyber Security · Rotterdam, Nederland
Het technische team geleid en nieuwe medewerkers ingewerkt en opgeleid tot het vereiste technische niveau.

2019

**Oprichter · CEO · CTO** · Secbiz IT Security GmbH

- Oprichter en technisch leider van een cybersecuritybedrijf.
- Onderzoek en advies over industriële/OT- en applicatiebeveiliging.
- Live SCADA-hackdemonstratie op de Hannover Messe in 2019.

## Veloce

Veloce is mijn JavaScript/TypeScript-runtime voor agentic coding: een doelplatform waarop coding agents complete applicaties kunnen maken die leesbaar, controleerbaar en direct uitvoerbaar zijn, zonder eerst npm-afhankelijkheden, frameworks, buildtooling en deployment-glue aan elkaar te hoeven knopen.

De runtime levert de belangrijke bouwstenen direct mee: een restrictieve sandbox en permissiemodel, HTTP-serving, SQLite en PostgreSQL met ORM en KV-store, browser- en desktopfuncties en packaging naar één zelfstandige native binary. Rekenintensieve paden kunnen vanuit JavaScript/TypeScript worden uitbesteed aan Rust-backed native kernels of WebAssembly. Het doel is software die agents betrouwbaar kunnen genereren, mensen nog steeds kunnen begrijpen en systemen met zo weinig mogelijk bewegende delen kunnen uitvoeren.

## Expertise

### Embedded, OT en medische technologie

Kwetsbaarheidsonderzoek in firmware en verbonden apparaten: brandmeldsystemen, industriële besturingen (SCADA), ziekenhuis- en medische apparatuur.

### Exploitontwikkeling

Van een afzonderlijke memory-corruption-kwetsbaarheid tot een volledige exploitketen met remote root-toegang.

### Browser- en webbeveiliging

SOP/CORS-bypasses, aanvalspaden naar apparaten op interne netwerken, XSS en applicatiebeveiliging.

### Responsible disclosure

Melden en afstemmen met fabrikanten en beheerders, van grote ondernemingen tot gemeentelijke overheden, inclusief ondersteuning bij herstel.

### Eigen tooling

Tooling en automatisering voor kwetsbaarheidsdetectie en pentesting, inclusief AI-ondersteunde workflows. Auteur van de JavaScript/TypeScript-runtime Veloce.

## Onderzoek

| Jaar | Onderzoek / kwetsbaarheid | Bron |
|---|---|---|
| 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-vermelding bij CIRCL |
| 2013 | Apple Motion - CVE-2013-6114 - kwetsbaarheid | Apple |
| 2014 | Apple Web Server - securityonderzoek, februari 2014 | Apple |
| 2012 | Nokia Hall of Fame - securityonderzoek, december 2012 | Nokia |
| 2012 | Android Browser DoS - CVE-2012-6301 - Metasploit-module | Rapid7 |
| 2012 | Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service | Bugtraq-archief |
| 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 |

| Jaar | Onderzoek / kwetsbaarheid | Bron |
|---|---|---|
| 2012 | plow .plowrc - Buffer Overflow - BID 54290 | Bugtraq |
| 2012 | Internet Explorer - XSS Filter Bypass - Exploit-DB 22100 | VulDB |

## Media

| Jaar | Oorspronkelijk artikel | Medium |
|---|---|---|
| 2025 | Verslaggeving over responsible disclosure bij Securitas / Marvelit | Security-Insider |
| 2022 | Radio-item over cybersecurity en ethisch hacken | WDR |
| 2024 | ÖAG-expertgesprek: Veiligheid 4.0 - cybersecurity en AI-verdediging | medianet (Oostenrijk) |
| 2024 | Beveiligingslekken in ziekenhuizen: patiënten in gevaar | Golem |
| 2024 | Browser-SOP/CORS en apparaten op het interne netwerk | CYTRES Research |
| 2024 | Openbare beveiligingsmelding van Jean Pereira met gedocumenteerde update over de oplossing | Volksbank / Sparda Bank (Responsible Disclosure) |
| 2023 | Expertgesprek met staatssecretaris Tursky over digitalisering, AI en cybersecurity | KURIER (Oostenrijk) |
| 2023 | Deelname als cybersecurity-expert aan de ÖAG Super Tuesday | LEADERSNET (Oostenrijk) |
| 2022 | Podcast #51: Ethical Hacker - securityonderzoek en loopbaan | IDG TechTalk / COMPUTERWOCHE |
| 2022 | IT-beveiligingslek bij de gemeente Keulen | Kölner Stadt-Anzeiger |
| 2022 | Privacycommissaris onderzoekt genegeerde melding van beveiligingslek | WirtschaftsWoche |
| 2022 | Responsible disclosure / 45 organisaties | Golem |
| 2022 | Bericht over OBI en overheidsinstanties | connect professional |
| 2020 | Keynote over browser- en applicatiebeveiliging | OMT - Online Marketing Konferenz |
| 2019 | Industrial Security Forum: live SCADA/ICS-hacking | Hannover Messe / MittelstandsWiki |
| 2019 | Interview "We hebben meer hackers nodig" | atp magazin |
| 2019 | Cyberaanvallen & darknet - Jean Pereira in interview | Podcast "IT'S IN YOU" |
| 2018 | SEO-DAY: Chrome hacken en SSL omzeilen in 2018 | Host Europe |
| 2018 | Beveiligingspresentatie in het superpanel van SEO-DAY 2018 | SEO-DAY / Online-Profession |
| 2018 | International Cyber Security Conference: Ethical Hacker en SECBIZ-oprichter in de sprekerslijst | DSS IT SEC / Riga |