# Jean Pereira

Pesquisa de segurança · Segurança ofensiva · Engenharia full-stack

Investigo vulnerabilidades em sistemas complexos e desenvolvo software de segurança e produtos próprios nas áreas de segurança de navegadores, sistemas embarcados e industriais, automação e IA.

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

## Perfil

Encontro vulnerabilidades de segurança onde outros deixam de procurar e desenvolvo software seguro que resolve problemas complexos.

Meu trabalho inclui vulnerabilidades em produtos e tecnologias da **Siemens**, **Apple**, **Google**, **Microsoft** e **Nokia**, além de diversos projetos na área de tecnologia médica. Atualmente, meu foco está na pesquisa em segurança e na engenharia de software.

Também sou autor do **Veloce**. Podes contactar-me através do formulário de contacto ou diretamente no LinkedIn.

## Destaques

### Quatro zero-days na Siemens: sistemas de alarme e detetores de incêndio controlados à distância

Assumi remotamente o controlo completo de sistemas de alarme e detetores de incêndio da Siemens. O meu exploit concedeu-me acesso root, os privilégios máximos do sistema, sem credenciais, cliques ou outra intervenção da vítima.

Desenvolvi uma cadeia de exploração combinando quatro vulnerabilidades desconhecidas e demonstrei a tomada de controlo na prática. Estava em causa o controlo de tecnologia de alarme essencial à segurança.

A Siemens confirmou os quatro resultados, CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. O exploit recebeu CVSS 10.0, a criticidade máxima possível.

### Zero-days em hospitais: grupos sanguíneos manipulados, alarmes ECG e equipamentos de ventilação ambiental desativados

Numa avaliação de segurança descobri 22 vulnerabilidades desconhecidas em dispositivos de doze fabricantes e demonstrei os ataques com exploits funcionais: desativar alarmes ECG, interromper a ventilação de blocos operatórios estéreis e manipular grupos sanguíneos e registos de alergias. Desenvolvi também bypasses SOP/CORS para demonstrar ataques remotos a dispositivos internos não acessíveis diretamente pela Internet.

Os fabricantes investigados incluem ZEISS, MOXA, Zebra, Dedalus Labor e Tetronik. Segundo a reportagem da Golem de 2024, os dispositivos afetados eram utilizados em milhares de outros hospitais e instituições médicas. Coordenei a divulgação e apoiei a correção. Jornalistas acompanharam todo o processo, desde a notificação aos fabricantes até ao meu apoio à correção.

### Vulnerabilidades em mais de 40 entidades públicas, na OBI, na REWE e no Instituto Fraunhofer

Descobri vulnerabilidades em 45 autarquias e empresas e comuniquei-as aos responsáveis. Na OBI, uma vulnerabilidade web permitia sequestrar sessões e aceder a informações do sistema interno de gestão de conteúdos.

Muitas autarquias corrigiram as falhas. A OBI retirou o site afetado após a controvérsia pública. A Golem e a WirtschaftsWoche documentaram a investigação e as respostas das empresas.

## Experiência

jun. de 2023 - presente

**CEO · CTO** · CYTRES GmbH
Fundei e liderei a empresa com foco em desenvolvimento de software e pesquisa em cibersegurança.

dez. de 2016 - ago. de 2019

**Tutor de cibersegurança** · CIC (Cambridge Innovation Center) · Rotterdam, Países Baixos
Ministrei workshops de cibersegurança e treinamentos técnicos.

dez. de 2016 - ago. de 2019

**Consultor sênior de segurança** · Base Cyber Security · Rotterdam, Países Baixos
Liderei a equipe técnica e treinei novos colaboradores até o padrão técnico exigido.

2019

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

- Fundador e líder técnico de uma empresa de segurança da informação.
- Pesquisa e consultoria em segurança industrial/OT e aplicações.
- Demonstração ao vivo de exploração de SCADA na Hannover Messe 2019.

## Veloce

Veloce é o meu runtime JavaScript/TypeScript para programação agêntica: uma plataforma-alvo na qual agentes de código podem criar aplicações completas, legíveis, auditáveis e prontas para executar, sem precisar montar antes dependências npm, frameworks, ferramentas de build e camadas de deployment.

O runtime já traz os blocos essenciais: sandbox e modelo de permissões restritivos, servidor HTTP, SQLite e PostgreSQL com ORM e armazenamento KV, recursos de navegador e desktop e empacotamento em um binário nativo autônomo. Caminhos de computação intensiva podem ser movidos de JavaScript/TypeScript para kernels nativos baseados em Rust ou WebAssembly. O objetivo é software que agentes consigam gerar com confiabilidade, que pessoas ainda consigam entender e que sistemas executem com o mínimo possível de partes móveis.

## Competências

**Sistemas embarcados, OT e dispositivos médicos**

Pesquisa de vulnerabilidades em firmware e dispositivos conectados: sistemas de alarme de incêndio, controladores industriais (SCADA), equipamentos hospitalares e médicos.

**Desenvolvimento de exploits**

De uma falha isolada de corrupção de memória a uma cadeia completa de exploração com acesso root remoto.

**Segurança de navegador e web**

Bypasses de SOP/CORS, caminhos de ataque para dispositivos em redes internas, XSS e segurança de aplicações.

**Divulgação responsável**

Relato e coordenação com fabricantes e operadores, de grandes empresas a administrações municipais, incluindo apoio à correção.

**Ferramentas próprias**

Ferramentas e automação para descoberta de vulnerabilidades e testes de penetração, incluindo fluxos assistidos por IA. Autor da runtime JavaScript/TypeScript Veloce.

## Pesquisa

| Ano | Pesquisa / vulnerabilidade | 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 | entrada da CISA no CIRCL |
| 2013 | Apple Motion - CVE-2013-6114 - vulnerabilidade | Apple |
| 2014 | Apple Web Server - pesquisa de segurança, fevereiro de 2014 | Apple |
| 2012 | Nokia Hall of Fame - pesquisa de segurança, dezembro de 2012 | Nokia |
| 2012 | Android Browser DoS - CVE-2012-6301 - módulo Metasploit | Rapid7 |
| 2012 | Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service | arquivo 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 |

| Ano | Pesquisa / vulnerabilidade | Fonte |
|---|---|---|
| 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 |

## Imprensa

| Ano | Publicação original | Veículo |
|---|---|---|
| 2025 | Cobertura sobre divulgação responsável na Securitas / Marvelit | Security-Insider |
| 2022 | Participação em rádio sobre cibersegurança e hacking ético | WDR |
| 2024 | Debate de especialistas da ÖAG: Segurança 4.0 - cibersegurança e defesa com IA | medianet (Áustria) |
| 2024 | Vulnerabilidades de segurança em hospitais: pacientes em risco | Golem |
| 2024 | SOP/CORS do navegador e dispositivos da rede interna | CYTRES Research |
| 2024 | Aviso público de segurança de Jean Pereira com atualização documentada da correção | Volksbank / Sparda Bank (Responsible Disclosure) |
| 2023 | Debate com o secretário de Estado Tursky sobre digitalização, IA e cibersegurança | KURIER (Áustria) |
| 2023 | Participação como especialista em cibersegurança no ÖAG Super Tuesday | LEADERSNET (Áustria) |
| 2022 | Podcast #51: Ethical Hacker - pesquisa de segurança e trajetória profissional | IDG TechTalk / COMPUTERWOCHE |
| 2022 | Vulnerabilidade de segurança de TI na cidade de Colônia | Kölner Stadt-Anzeiger |
| 2022 | A comissária de proteção de dados investiga uma vulnerabilidade de segurança relatada e ignorada | WirtschaftsWoche |
| 2022 | Divulgação responsável / 45 organizações | Golem |
| 2022 | Reportagem sobre a OBI e órgãos públicos | connect professional |
| 2020 | Keynote sobre segurança de navegadores e aplicações | OMT - Online Marketing Konferenz |
| 2019 | Industrial Security Forum: hacking SCADA/ICS ao vivo | Hannover Messe / MittelstandsWiki |
| 2019 | Entrevista "Precisamos de mais hackers" | atp magazin |
| 2019 | Ciberataques e darknet - entrevista com Jean Pereira | Podcast "IT'S IN YOU" |
| 2018 | SEO-DAY: como hackear o Chrome e contornar SSL em 2018 | Host Europe |
| 2018 | Palestra sobre segurança no superpanel do SEO-DAY 2018 | SEO-DAY / Online--Profession |
| 2018 | International Cyber Security Conference: Ethical Hacker e fundador da SECBIZ entre os palestrantes | DSS IT SEC / Riga |