Jean Pereira

보안 연구 · 공격 보안 · 풀스택 엔지니어링

복잡한 시스템의 취약점을 연구하고 브라우저 보안, 임베디드 및 산업 시스템, 자동화, AI 분야의 보안 소프트웨어와 자체 제품을 개발합니다.

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

프로필

다른 사람들이 찾기를 멈춘 곳에서 보안 취약점을 발견하고, 복잡한 문제를 해결하는 안전한 소프트웨어를 만듭니다.

제 작업에는 **Siemens**, **Apple**, **Google**, **Microsoft**, **Nokia**의 제품과 기술에서 발견한 취약점과 의료기술 분야의 다양한 프로젝트가 포함됩니다. 현재 보안 연구와 소프트웨어 엔지니어링에 집중하고 있습니다.

또한 **Veloce**의 개발자입니다. 문의 양식을 이용하거나 LinkedIn에서 직접 연락하실 수 있습니다.

하이라이트

Siemens의 제로데이 **4**개: 경보 시스템과 화재 감지기를 원격으로 장악

Siemens 경보 시스템과 화재 감지기를 원격으로 완전히 장악했습니다. 제 익스플로잇은 장치의 최고 시스템 권한인 root 접근 권한을 확보했습니다. 로그인 정보, 클릭 또는 피해자의 어떠한 참여도 필요하지 않았습니다.

알려지지 않은 취약점 4개를 연결한 익스플로잇 체인을 개발하고 완전한 장악을 실제로 입증했습니다. 안전에 핵심적인 경보 기술의 제어권에 관한 결과입니다.

Siemens는 네 발견을 CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904로 확인했습니다. 익스플로잇은 CVSS 10.0으로 평가되었으며, 가능한 최대 심각도를 뜻합니다.

병원의 제로데이: 혈액형 조작, **ECG** 경보와 환기 장치 중단 입증

보안 평가에서 제조사 12곳의 장치에서 알려지지 않은 취약점 22개를 발견하고 작동하는 익스플로잇으로 공격을 입증했습니다. ECG 경보 비활성화, 무균 수술실 환기 중단, 혈액형과 알레르기 기록 조작이 포함됩니다. 자체 SOP/CORS 우회 기법으로 인터넷에서 직접 접근할 수 없는 내부 장치에 대한 원격 공격도 입증했습니다.

조사한 제조사에는 ZEISS, MOXA, Zebra, Dedalus Labor, Tetronik이 포함됩니다. Golem의 2024년 보도에 따르면 해당 장치는 수천 곳의 다른 병원과 의료 시설에도 사용되고 있었습니다. 제조사에 대한 공개를 조율하고 수정을 지원했습니다. 제조사에 대한 신고부터 수정 지원까지 전 과정을 기자들이 동행 취재했습니다.

40곳 이상의 공공기관, **OBI, REWE** 및 프라운호퍼 연구소의 취약점

45개 지방자치단체와 기업에서 취약점을 발견하고 담당자에게 신고했습니다. OBI의 웹 취약점은 사용자 세션 탈취와 내부 콘텐츠 관리 시스템 정보 접근을 가능하게 했습니다.

많은 지자체가 문제를 수정했습니다. OBI는 공개 논쟁 후 해당 웹사이트를 중단했습니다. Golem과 WirtschaftsWoche는 연구와 기업들의 대응을 보도했습니다.

경력

2023년 6월 - 현재

CEO · CTO · CYTRES GmbH
소프트웨어 개발과 사이버보안 연구에 중점을 두고 회사를 설립하고 이끌었습니다.

2016년 12월 - 2019년 8월

사이버보안 튜터 · CIC (Cambridge Innovation Center) · Rotterdam, 네덜란드
사이버보안 워크숍과 기술 교육을 진행했습니다.

2016년 12월 - 2019년 8월

수석 보안 자문역 · Base Cyber Security · Rotterdam, 네덜란드
기술팀을 이끌고 신규 직원이 요구되는 기술 수준에 도달하도록 교육했습니다.

2019

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

- 사이버보안 기업 창업자 및 기술 책임자.
- 산업/OT 및 애플리케이션 보안 연구와 컨설팅.
- Hannover Messe 2019에서 SCADA 해킹 라이브 시연.

Veloce

Veloce는 agentic coding을 위해 제가 개발한 JavaScript/TypeScript 런타임입니다. 코딩 에이전트가 npm 의존성, 프레임워크, 빌드 도구, 배포용 glue를 먼저 조립하지 않고도 읽기 쉽고 감사 가능하며 바로 실행할 수 있는 완성형 애플리케이션을 만들 수 있는 대상 플랫폼입니다.

런타임에는 핵심 구성 요소가 기본으로 포함됩니다. 제한적인 sandbox와 permission 모델, HTTP 서버, ORM과 KV 저장소를 포함한 SQLite/PostgreSQL, 브라우저 및 데스크톱 기능, 그리고 독립 실행형 native binary 패키징입니다. 계산 집약적인 경로는 JavaScript/TypeScript에서 Rust 기반 native kernel이나 WebAssembly로 넘길 수 있습니다. 목표는 에이전트가 안정적으로 생성하고, 사람이 계속 이해할 수 있으며, 시스템이 가능한 한 적은 moving parts로 실행할 수 있는 소프트웨어입니다.

전문 분야

임베디드, OT 및 의료기기

펌웨어와 연결 장치의 취약점 연구: 화재 경보 시스템, 산업용 제어기(SCADA), 병원 및 의료 장비.

Exploit 개발

단일 memory corruption 버그부터 원격 root 접근이 가능한 전체 exploit chain까지.

브라우저 및 웹 보안

SOP/CORS 우회, 내부 네트워크 장치로 이어지는 공격 경로, XSS 및 애플리케이션 보안.

책임 있는 공개

대기업부터 지방 행정기관까지 제조사 및 운영자와 신고 및 조율을 진행하고 수정 과정도 지원합니다.

자체 도구

취약점 발견 및 penetration testing을 위한 도구와 자동화, AI 지원 workflow 포함. JavaScript/TypeScript runtime Veloce의 제작자.

연구

연도	연구 / 취약점	출처
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	CIRCL의 CISA 항목
2013	Apple Motion - CVE-2013-6114 - 보안 취약점	Apple
2014	Apple Web Server - 보안 연구, 2014년 2월	Apple
2012	Nokia Hall of Fame - 보안 연구, 2012년 12월	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit 모듈	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq 아카이브
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

언론

연도	원문	매체
2025	Securitas / Marvelit의 책임 있는 공개 관련 보도	Security-Insider
2022	사이버 보안과 윤리적 해킹에 관한 라디오 프로그램	WDR
2024	ÖAG 전문가 토크: 보안 4.0 - 사이버 보안과 AI 방어	medianet (오스트리아)
2024	병원 보안 취약점: 환자 위험	Golem
2024	브라우저 SOP/CORS 및 내부 네트워크 장치	CYTRES Research
2024	Jean Pereira의 공개 보안 공지와 문서화된 수정 업데이트	Volksbank / Sparda Bank (Responsible Disclosure)
2023	투르스키 국무차관과 디지털화, AI, 사이버 보안에 관한 전문가 토크	KURIER (오스트리아)
2023	ÖAG Super Tuesday에 사이버 보안 전문가로 참여	LEADERSNET (오스트리아)
2022	팟캐스트 #51: Ethical Hacker - 보안 연구와 경력	IDG TechTalk / COMPUTERWOCHE
2022	쾰른 시의 IT 보안 취약점	Kölner Stadt-Anzeiger
2022	신고된 보안 취약점이 무시되자 개인정보 보호 위원이 조사에 착수	WirtschaftsWoche
2022	책임 있는 공개 / 45개 조직	Golem
2022	OBI와 공공기관에 관한 보도	connect professional
2020	브라우저 및 애플리케이션 보안 기조연설	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: SCADA/ICS 라이브 해킹	Hannover Messe / MittelstandsWiki
2019	인터뷰 "더 많은 해커가 필요하다"	atp magazin
2019	사이버 공격과 다크넷 - Jean Pereira 인터뷰	Podcast "IT'S IN YOU"
2018	SEO-DAY: 2018년 Chrome을 해킹하고 SSL을 우회하는 방법	Host Europe
2018	SEO-DAY 2018 슈퍼패널 보안 강연	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker 및 SECBIZ 창립자가 연사로 참여	DSS IT SEC / Riga