Jean Pereira

Badania bezpieczeństwa · Bezpieczeństwo ofensywne · Inżynieria full-stack

Badam podatności w złożonych systemach oraz tworzę oprogramowanie bezpieczeństwa i własne produkty z obszaru bezpieczeństwa przeglądarek, systemów wbudowanych i przemysłowych, automatyzacji oraz AI.

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

Profil

Znajduję luki bezpieczeństwa tam, gdzie inni przestają szukać, i tworzę bezpieczne oprogramowanie, które rozwiązuje złożone problemy.

Moja praca obejmuje podatności w produktach i technologiach **Siemens**, **Apple**, **Google**, **Microsoft** i **Nokia**, a także różne projekty w dziedzinie technologii medycznych. Obecnie skupiam się na badaniach bezpieczeństwa i inżynierii oprogramowania.

Jestem również autorem **Veloce**. Możesz się ze mną skontaktować przez formularz kontaktowy lub bezpośrednio na LinkedIn.

Najważniejsze

Cztery luki zero-day w Siemens: systemy alarmowe i czujki pożarowe przejęte zdalnie

Zdalnie przejąłem pełną kontrolę nad systemami alarmowymi i czujkami pożarowymi Siemens. Mój exploit zapewnił dostęp root, czyli najwyższe uprawnienia systemowe, bez danych logowania, kliknięć i innych działań ofiary.

Opracowałem łańcuch exploitów łączący cztery nieznane luki i praktycznie zademonstrowałem pełne przejęcie. Chodziło o kontrolę nad techniką alarmową kluczową dla bezpieczeństwa.

Siemens potwierdził cztery odkrycia jako CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Exploit otrzymał ocenę CVSS 10.0, maksymalna możliwa krytyczność.

Zero-day w szpitalach: grupy krwi zmienione, alarmy EKG i urządzenia wentylacyjne wyłączone

Podczas audytu odkryłem 22 nieznane wcześniej luki w urządzeniach dwunastu producentów i zademonstrowałem ataki działającymi exploitami: wyłączanie alarmów EKG, przerywanie wentylacji sterylnych sal operacyjnych oraz manipulowanie grupami krwi i danymi o alergiach. Opracowałem też obejścia SOP/CORS, demonstrując zdalne ataki na urządzenia wewnętrzne niedostępne bezpośrednio z Internetu.

Badani producenci to m.in. ZEISS, MOXA, Zebra, Dedalus Labor i Tetronik. Według reportażu Golem z 2024 r. urządzenia te działały w tysiącach innych szpitali i placówek medycznych. Koordynowałem zgłoszenia i wspierałem usuwanie luk. Dziennikarze śledzili cały proces, od zgłoszenia producentom po moje wsparcie przy usuwaniu luk.

Luki w ponad 40 urzędach, OBI, REWE i Instytucie Fraunhofera

Odkryłem luki w 45 urzędach miejskich i firmach oraz zgłosiłem je odpowiedzialnym zespołom. W OBI luka internetowa umożliwiała przejmowanie sesji użytkowników i odczyt informacji z wewnętrznego systemu zarządzania treścią.

Wiele urzędów usunęło zgłoszone luki. OBI wyłączyło stronę po publicznym sporze. Golem i WirtschaftsWoche udokumentowały badania oraz reakcje firm.

Doświadczenie

cze 2023 - obecnie

CEO · CTO · CYTRES GmbH
Założyłem i prowadziłem firmę, koncentrując się na tworzeniu oprogramowania i badaniach cyberbezpieczeństwa.

gru 2016 - sie 2019

Tutor cyberbezpieczeństwa · CIC (Cambridge Innovation Center) · Rotterdam, Holandia
Prowadziłem warsztaty z cyberbezpieczeństwa i szkolenia techniczne.

gru 2016 - sie 2019

Starszy doradca ds. bezpieczeństwa · Base Cyber Security · Rotterdam, Holandia
Kierowałem zespołem technicznym oraz wdrażałem i szkoliłem nowych pracowników do wymaganego poziomu technicznego.

2019

Założyciel · CEO · CTO · Secbiz IT Security GmbH

- Założyciel i lider techniczny firmy cyberbezpieczeństwa.
- Badania i doradztwo w zakresie bezpieczeństwa przemysłowego/OT oraz aplikacji.
- Pokaz włamania do SCADA na Hannover Messe 2019.

Veloce

Veloce to mój runtime JavaScript/TypeScript do agentic coding: platforma docelowa, na której agenci programistyczni mogą tworzyć kompletne aplikacje, czytelne, możliwe do audytu i od razu uruchamialne, bez wcześniejszego składania zależności npm, frameworków, narzędzi build i warstwy wdrożeniowej.

Runtime zawiera najważniejsze elementy w standardzie: restrykcyjny sandbox i model uprawnień, serwer HTTP, SQLite i PostgreSQL z ORM i magazynem KV, funkcje przeglądarkowe i desktopowe oraz pakowanie do samodzielnego natywnego pliku binarnego. Obciążające obliczeniowo fragmenty można przenieść z JavaScript/TypeScript do natywnych kerneli opartych na Rust lub WebAssembly. Celem jest oprogramowanie, które agenci generują niezawodnie, ludzie nadal rozumieją, a systemy uruchamiają z minimalną liczbą ruchomych części.

Kompetencje

Systemy wbudowane, OT i urządzenia medyczne

Badania podatności w firmware i urządzeniach sieciowych: systemy alarmów pożarowych, sterowniki przemysłowe (SCADA), sprzęt szpitalny i medyczny.

Tworzenie exploitów

Od pojedynczego błędu memory corruption do pełnego łańcucha exploitów ze zdalnym dostępem root.

Bezpieczeństwo przeglądarek i web

Obejścia SOP/CORS, ścieżki ataku do urządzeń w sieciach wewnętrznych, XSS i bezpieczeństwo aplikacji.

Odpowiedzialne ujawnianie

Zgłaszanie i koordynacja z producentami i operatorami, od dużych firm po administracje miejskie, wraz ze wsparciem przy usuwaniu problemów.

Własne narzędzia

Narzędzia i automatyzacja do wykrywania podatności i testów penetracyjnych, w tym workflow wspierane przez AI. Autor środowiska JavaScript/TypeScript Veloce.

Badania

Rok	Badania / podatność	Źródło
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	wpis CISA w CIRCL
2013	Apple Motion - CVE-2013-6114 - podatność	Apple
2014	Apple Web Server - badania bezpieczeństwa, luty 2014	Apple
2012	Nokia Hall of Fame - badania bezpieczeństwa, grudzień 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - moduł Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	archiwum 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
2012	DomsHttpd - Remote Denial of Service - BID 54478	Bugtraq
2012	CommPort - SQL Injection - BID 55239	Bugtraq
2012	Arctic Torrent - Memory Corruption - BID 55833	Bugtraq

Rok	Badania / podatność	Źródło
2012	plow .plowrc - Buffer Overflow - BID 54290	Bugtraq
2012	Internet Explorer - XSS Filter Bypass - Exploit-DB 22100	VulDB

Media

Rok	Oryginalny artykuł	Medium
2025	Relacja dotycząca responsible disclosure w Securitas / Marvelit	Security-Insider
2022	Audycja radiowa o cyberbezpieczeństwie i etycznym hackingu	WDR
2024	Debata ekspertów ÖAG: Bezpieczeństwo 4.0 - cyberbezpieczeństwo i obrona z użyciem AI	medianet (Austria)
2024	Luki bezpieczeństwa w szpitalach: pacjenci w niebezpieczeństwie	Golem
2024	SOP/CORS przeglądarki i urządzenia w sieci wewnętrznej	CYTRES Research
2024	Publiczne zgłoszenie bezpieczeństwa Jeana Pereiry z udokumentowaną aktualizacją dotyczącą usunięcia problemu	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Debata z sekretarzem stanu Turskym o cyfryzacji, AI i cyberbezpieczeństwie	KURIER (Austria)
2023	Udział jako ekspert ds. cyberbezpieczeństwa w ÖAG Super Tuesday	LEADERSNET (Austria)
2022	Podcast #51: Ethical Hacker - badania bezpieczeństwa i droga zawodowa	IDG TechTalk / COMPUTERWOCHE
2022	Luka bezpieczeństwa IT w administracji miasta Kolonia	Kölner Stadt-Anzeiger
2022	Komisarz ds. ochrony danych prowadzi dochodzenie w sprawie zignorowanej zgłoszonej luki bezpieczeństwa	WirtschaftsWoche
2022	Responsible disclosure / 45 organizacji	Golem
2022	Relacja dotycząca OBI i administracji publicznej	connect professional
2020	Keynote o bezpieczeństwie przeglądarek i aplikacji	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: hakowanie SCADA/ICS na żywo	Hannover Messe / MittelstandsWiki
2019	Wywiad "Potrzebujemy więcej hakerów"	atp magazin
2019	Cyberataki i darknet - wywiad z Jeanem Pereirą	Podcast "IT'S IN YOU"
2018	SEO-DAY: jak zhakować Chrome i obejść SSL w 2018 roku	Host Europe
2018	Prelekcja o bezpieczeństwie w superpanelu SEO-DAY 2018	SEO-DAY / Online--Profession
2018	International Cyber Security Conference: Ethical Hacker i założyciel SECBIZ w gronie prelegentów	DSS IT SEC / Riga