Jean Pereira

Дослідження безпеки · Наступальна безпека · Full-stack розробка

Я досліджую вразливості складних систем і розробляю програмне забезпечення для безпеки та власні продукти у сферах безпеки браузерів, вбудованих і промислових систем, автоматизації та ШІ.

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

Профіль

Я знаходжу вразливості там, де інші припиняють шукати, і створюю безпечне програмне забезпечення, що розв'язує складні завдання.

Моя робота охоплює вразливості в продуктах і технологіях **Siemens**, **Apple**, **Google**, **Microsoft** і **Nokia**, а також різні проєкти у сфері медичної техніки. Зараз я зосереджуюся на дослідженнях безпеки та розробці програмного забезпечення.

Я також автор **Veloce**. Зі мною можна зв'язатися через контактну форму або безпосередньо в LinkedIn.

Головне

Чотири zero-day у Siemens: системи сигналізації та пожежні сповіщувачі захоплено віддалено

Я віддалено отримав повний контроль над системами сигналізації та пожежними сповіщувачами Siemens. Мій експлойт надав доступ root, тобто найвищі системні привілеї, без облікових даних, кліків або інших дій жертви.

Я розробив ланцюжок експлуатації чотирьох невідомих вразливостей і практично продемонстрував повне захоплення. Ішлося про контроль над критично важливою для безпеки сигнальною технікою.

Siemens підтвердила чотири знахідки: CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Експлойт отримав оцінку CVSS 10.0, що означає максимально можливу критичність.

Zero-day у лікарнях: групи крові підмінено, тривоги ЕКГ та вентиляційні установки вимкнено

Під час дослідження безпеки я виявив 22 раніше невідомі вразливості у пристроях дванадцяти виробників і продемонстрував атаки робочими експлойтами: вимкнення тривог ЕКГ, зупинку вентиляції стерильних операційних і зміну груп крові та даних про алергії. Розроблені мною обходи SOP/CORS також дали змогу продемонструвати віддалені атаки на внутрішні пристрої без прямого доступу з інтернету.

Серед досліджених виробників ZEISS, MOXA, Zebra, Dedalus Labor і Tetronik. За репортажем Golem 2024 року, пристрої використовувалися в тисячах інших лікарень і медичних закладів. Я координував повідомлення виробникам і супроводжував виправлення. Журналісти супроводжували весь процес: від повідомлення виробникам до моєї допомоги в усуненні вразливостей.

Вразливості у понад 40 органах влади, OBI, REWE та Інституті Фраунгофера

Я виявив вразливості у 45 муніципалітетах і компаніях та повідомив відповідальним. В OBI вебвразливість дозволяла перехоплювати користувацькі сесії та читати інформацію з внутрішньої системи керування вмістом.

Багато муніципалітетів виправили помилки. OBI вимкнула сайт після публічної суперечки. Golem і WirtschaftsWoche задокументували дослідження та реакції компаній.

Досвід

черв. 2023 р. - дотепер

CEO · CTO · CYTRES GmbH
Заснував і очолював компанію з фокусом на розробці програмного забезпечення та дослідженнях кібербезпеки.

груд. 2016 р. - серп. 2019 р.

Викладач із кібербезпеки · CIC (Cambridge Innovation Center) · Rotterdam, Нідерланди
Проводив воркшопи з кібербезпеки та технічні навчання.

груд. 2016 р. - серп. 2019 р.

Старший радник із безпеки · Base Cyber Security · Rotterdam, Нідерланди
Керував технічною командою та навчав нових співробітників до необхідного технічного рівня.

2019

Засновник · CEO · CTO · Secbiz IT Security GmbH
- Засновник і технічний керівник компанії з кібербезпеки.
- Дослідження та консультації з промислової/OT і прикладної безпеки.
- Жива демонстрація атак на SCADA на Hannover Messe 2019.

Veloce

Veloce - мій JavaScript/TypeScript runtime для agentic coding: цільова платформа, на якій програмні агенти можуть створювати повноцінні застосунки, що залишаються читабельними, придатними до аудиту й одразу запускаються без попереднього складання npm-залежностей, фреймворків, build-інструментів і deployment glue.

Runtime одразу містить ключові компоненти: обмежувальний sandbox і модель permissions, HTTP-сервер, SQLite та PostgreSQL з ORM і KV-сховищем, браузерні й desktop-можливості та пакування в самостійний native binary. Обчислювально важкі частини можна переносити з JavaScript/TypeScript у native kernels на Rust або WebAssembly. Мета - ПЗ, яке агенти можуть надійно генерувати, люди й надалі розуміти, а системи запускати з мінімумом рухомих частин.

Компетенції

Вбудовані системи, OT і медична техніка

Дослідження вразливостей у прошивках і підключених пристроях: системи пожежної сигналізації, промислові контролери (SCADA), лікарняне та медичне обладнання.

Розробка експлойтів

Від окремої помилки memory corruption до повного ланцюжка експлуатації з віддаленим root-доступом.

Безпека браузерів і web

Обходи SOP/CORS, шляхи атаки до пристроїв у внутрішніх мережах, XSS і безпека застосунків.

Відповідальне розкриття

Повідомлення та координація з виробниками й операторами, від великих компаній до муніципальних адміністрацій, включно з підтримкою виправлення.

Власні інструменти

Інструменти та автоматизація для пошуку вразливостей і penetration testing, включно з workflow за підтримки ШІ. Автор JavaScript/TypeScript runtime Veloce.

Дослідження

Рік	Дослідження / вразливість	Джерело
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	запис CISA у CIRCL
2013	Apple Motion - CVE-2013-6114 - вразливість	Apple
2014	Apple Web Server - дослідження безпеки, лютий 2014 р.	Apple
2012	Nokia Hall of Fame - дослідження безпеки, грудень 2012 р.	Nokia
2012	Android Browser DoS - CVE-2012-6301 - модуль Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	архів 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

Рік	Дослідження / вразливість	Джерело
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

Преса

Рік	Оригінальна стаття	Видання
2025	Матеріал про відповідальне розкриття вразливостей у Securitas / Marvelit	Security-Insider
2022	Радіосюжет про кібербезпеку та етичний хакінг	WDR
2024	Експертна дискусія ÖAG: Безпека 4.0 - кібербезпека та захист за допомогою ШІ	medianet (Австрія)
2024	Вразливості безпеки в лікарнях: пацієнти під загрозою	Golem
2024	SOP/CORS браузера та пристрої внутрішньої мережі	CYTRES Research
2024	Публічне повідомлення про безпеку від Жана Перейри з документованим оновленням щодо виправлення	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Експертна розмова з державним секретарем Турскі про цифровізацію, ШІ та кібербезпеку	KURIER (Австрія)
2023	Участь в ÖAG Super Tuesday як експерта з кібербезпеки	LEADERSNET (Австрія)
2022	Подкаст #51: Ethical Hacker - дослідження безпеки та професійний шлях	IDG TechTalk / COMPUTERWOCHE
2022	Вразливість IT-безпеки в адміністрації Кельна	Kölner Stadt-Anzeiger
2022	Уповноважена із захисту даних розслідує проігнороване повідомлення про вразливість	WirtschaftsWoche
2022	Відповідальне розкриття / 45 організацій	Golem
2022	Матеріал про OBI та органи влади	connect professional
2020	Ключова доповідь про безпеку браузерів і застосунків	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: живий злам SCADA/ICS	Hannover Messe / MittelstandsWiki
2019	Інтерв'ю «Нам потрібно більше хакерів»	atp magazin
2019	Кібератаки й даркнет - інтерв'ю з Жаном Перейрою	Podcast "IT'S IN YOU"
2018	SEO-DAY: як зламати Chrome та обійти SSL у 2018 році	Host Europe
2018	Доповідь про безпеку в суперпанелі SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker і засновник SECBIZ серед спікерів	DSS IT SEC / Riga