Jean Pereira

Исследование безопасности · Offensive security · Full-stack разработка

Я исследую уязвимости сложных систем и разрабатываю программное обеспечение для безопасности и собственные продукты в областях безопасности браузеров, встроенных и промышленных систем, автоматизации и ИИ.

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

Профиль

Я нахожу уязвимости там, где другие прекращают искать, и создаю безопасное ПО, которое решает сложные задачи.

Моя работа включает уязвимости в продуктах и технологиях **Siemens**, **Apple**, **Google**, **Microsoft** и **Nokia**, а также различные проекты в области медицинской техники. Сейчас я сосредоточен на исследованиях безопасности и разработке программного обеспечения.

Я также автор **Veloce**. Со мной можно связаться через контактную форму или напрямую в LinkedIn.

Главное

Четыре zero-day в Siemens: системы сигнализации и пожарные извещатели захвачены удалённо

Я удалённо получил полный контроль над системами сигнализации и пожарными извещателями Siemens. Мой эксплойт дал доступ root, то есть высшие системные привилегии, без учётных данных, кликов или иных действий жертвы.

Я разработал цепочку эксплуатации четырёх неизвестных уязвимостей и практически продемонстрировал полный захват. Речь шла о контроле над критически важной для безопасности сигнальной техникой.

Siemens подтвердила четыре находки: CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Эксплойт получил оценку CVSS 10.0, означающую максимально возможную критичность.

Zero-day в больницах: группы крови подменены, сигналы ЭКГ и вентиляционные установки отключены

При исследовании безопасности я обнаружил 22 неизвестные ранее уязвимости в устройствах двенадцати производителей и продемонстрировал атаки работающими эксплойтами: отключение сигналов ЭКГ, остановку вентиляции стерильных операционных и изменение групп крови и сведений об аллергиях. Разработанные мной обходы SOP/CORS также позволили продемонстрировать удалённые атаки на внутренние устройства без прямого доступа из интернета.

Среди исследованных производителей ZEISS, MOXA, Zebra, Dedalus Labor и Tetronik. По репортажу Golem 2024 года, устройства использовались в тысячах других больниц и медицинских учреждений. Я координировал уведомление производителей и сопровождал исправления. Журналисты сопровождали весь процесс: от уведомления производителей до моей помощи в устранении уязвимостей.

Уязвимости в более чем 40 органах власти, OBI, REWE и Институте Фраунгофера

Я обнаружил уязвимости в 45 муниципалитетах и компаниях и сообщил ответственным. В OBI веб-уязвимость позволяла перехватывать пользовательские сессии и читать информацию из внутренней системы управления контентом.

Многие муниципалитеты исправили ошибки. OBI отключила сайт после публичного спора. Golem и WirtschaftsWoche задокументировали исследование и реакцию компаний.

Опыт

июнь 2023 г. - н. в.

CEO · CTO · CYTRES GmbH
Основал и руководил компанией, сосредоточившись на разработке ПО и исследованиях кибербезопасности.

дек. 2016 г. - авг. 2019 г.

Преподаватель по кибербезопасности · CIC (Cambridge Innovation Center) · Rotterdam, Нидерланды
Проводил семинары по кибербезопасности и техническое обучение.

дек. 2016 г. - авг. 2019 г.

Старший консультант по безопасности · Base Cyber Security · Rotterdam, Нидерланды
Руководил технической командой и обучал новых сотрудников до требуемого технического уровня.

2019

Основатель · CEO · CTO · Secbiz IT Security GmbH

- Основатель и технический руководитель компании по кибербезопасности.
- Исследования и консалтинг в области промышленной/OT и прикладной безопасности.
- Живая демонстрация взлома SCADA на Hannover Messe 2019.

Veloce

Veloce - мой JavaScript/TypeScript runtime для agentic coding: целевая платформа, на которой программные агенты могут создавать полноценные приложения, остающиеся читаемыми, проверяемыми и сразу запускаемыми, без предварительной сборки npm-зависимостей, фреймворков, build-инструментов и deployment glue.

Runtime сразу включает ключевые компоненты: ограничивающую sandbox-модель и permissions, HTTP-сервер, SQLite и PostgreSQL с ORM и KV-хранилищем, браузерные и desktop-возможности и упаковку в самостоятельный native binary. Вычислительно тяжёлые участки можно переносить из JavaScript/TypeScript в нативные kernels на Rust или WebAssembly. Цель - ПО, которое агенты могут надёжно генерировать, люди по-прежнему понимать, а системы запускать с минимальным количеством движущихся частей.

Компетенции

Встроенные системы, OT и медицинская техника

Исследование уязвимостей в прошивках и подключённых устройствах: системы пожарной сигнализации, промышленные контроллеры (SCADA), больничное и медицинское оборудование.

Разработка эксплойтов

От отдельной ошибки memory corruption до полной цепочки эксплуатации с удалённым root-доступом.

Безопасность браузеров и web

Обходы SOP/CORS, пути атаки к устройствам во внутренних сетях, XSS и безопасность приложений.

Ответственное раскрытие

Сообщение и координация с производителями и операторами, от крупных компаний до муниципальных администраций, включая поддержку при устранении проблем.

Собственные инструменты

Инструменты и автоматизация для поиска уязвимостей и penetration testing, включая рабочие процессы с поддержкой ИИ. Автор JavaScript/TypeScript runtime Veloce.

Исследования

Год	Исследование / уязвимость	Источник
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	запись CISA в CIRCL
2013	Apple Motion - CVE-2013-6114 - уязвимость	Apple
2014	Apple Web Server - исследование безопасности, февраль 2014 г.	Apple
2012	Nokia Hall of Fame - исследование безопасности, декабрь 2012 г.	Nokia
2012	Android Browser DoS - CVE-2012-6301 - модуль Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	архив 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

Год	Исследование / уязвимость	Источник
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

Пресса

Год	Оригинальная статья	Издание
2025	Материал об ответственном раскрытии уязвимостей в Securitas / Marvelit	Security-Insider
2022	Радиосюжет о кибербезопасности и этичном хакинге	WDR
2024	Экспертная дискуссия ÖAG: Безопасность 4.0 - кибербезопасность и защита с помощью ИИ	medianet (Австрия)
2024	Уязвимости в больницах: пациенты под угрозой	Golem
2024	SOP/CORS браузера и устройства внутренней сети	CYTRES Research
2024	Публичное уведомление о безопасности от Жана Перейры с документированным обновлением об устранении	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Экспертная беседа с государственным секретарём Турски о цифровизации, ИИ и кибербезопасности	KURIER (Австрия)
2023	Участие в ÖAG Super Tuesday в качестве эксперта по кибербезопасности	LEADERSNET (Австрия)
2022	Подкаст #51: Ethical Hacker - исследования безопасности и профессиональный путь	IDG TechTalk / COMPUTERWOCHE
2022	Уязвимость ИТ-безопасности в администрации Кёльна	Kölner Stadt-Anzeiger
2022	Уполномоченная по защите данных расследует проигнорированное сообщение об уязвимости	WirtschaftsWoche
2022	Ответственное раскрытие / 45 организаций	Golem
2022	Материал об OBI и государственных органах	connect professional
2020	Ключевой доклад о безопасности браузеров и приложений	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: живой взлом SCADA/ICS	Hannover Messe / MittelstandsWiki
2019	Интервью «Нам нужно больше хакеров»	atp magazin
2019	Кибератаки и даркнет - интервью с Жаном Перейрой	Podcast "IT'S IN YOU"
2018	SEO-DAY: как взломать Chrome и обойти SSL в 2018 году	Host Europe
2018	Доклад по безопасности на суперпанели SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker и основатель SECBIZ среди спикеров	DSS IT SEC / Riga