Jean Pereira

নিরাপত্তা গবেষণা · Offensive Security · Full-Stack Engineering

আমি জটিল সিস্টেমের vulnerability নিয়ে গবেষণা করি এবং browser security, embedded ও industrial system, automation এবং AI-এর জন্য security software ও নিজস্ব product তৈরি করি।

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

প্রোফাইল

অন্যরা যেখানে খোঁজা থামিয়ে দেয়, আমি সেখানে নিরাপত্তার দুর্বলতা খুঁজে পাই এবং জটিল সমস্যার সমাধান করে এমন নিরাপদ সফটওয়্যার তৈরি করি।

আমার কাজের মধ্যে **Siemens**, **Apple**, **Google**, **Microsoft** ও **Nokia**-র product ও technology-তে vulnerability এবং চিকিৎসা প্রযুক্তিবিষয়ক বিভিন্ন প্রকল্প রয়েছে। বর্তমানে আমার মনোযোগ নিরাপত্তা গবেষণা ও সফটওয়্যার প্রকৌশলে।

আমি **Veloce**-এর নির্মাতাও। তুমি যোগাযোগের ফর্ম দিয়ে অথবা সরাসরি LinkedIn-এ আমার সঙ্গে যোগাযোগ করতে পারো।

মূল বিষয়গুলো

Siemens-এ চারটি জিরো-ডে: অ্যালার্ম ব্যবস্থা ও অগ্নি শনাক্তকারীর দূর থেকে নিয়ন্ত্রণ নেওয়া হয়েছে

আমি Siemens অ্যালার্ম ব্যবস্থা ও অগ্নি শনাক্তকারীর সম্পূর্ণ নিয়ন্ত্রণ দূর থেকে নিয়েছি। আমার এক্সপ্লয়েট root প্রবেশাধিকার, অর্থাৎ সর্বোচ্চ সিস্টেম অধিকার দিয়েছে। লগইন তথ্য, ক্লিক বা ভুক্তভোগীর কোনো অংশগ্রহণ প্রয়োজন হয়নি।

চারটি অজানা দুর্বলতা একত্র করে এক্সপ্লয়েট চেইন তৈরি করেছি এবং সম্পূর্ণ নিয়ন্ত্রণ বাস্তবে দেখিয়েছি। এটি নিরাপত্তার জন্য অত্যন্ত গুরুত্বপূর্ণ অ্যালার্ম প্রযুক্তির নিয়ন্ত্রণ।

Siemens চারটি আবিষ্কার CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904 হিসেবে নিশ্চিত করেছে। এক্সপ্লয়েটের মূল্যায়ন CVSS 10.0, অর্থাৎ সর্বাধিক সম্ভাব্য গুরুতরতা।

হাসপাতালে জিরো-ডে: রক্তের গ্রুপ বদলানো হয়েছে, **ECG** অ্যালার্ম ও বায়ু চলাচলের যন্ত্র বন্ধ করা হয়েছে

নিরাপত্তা মূল্যায়নে বারোটি প্রস্তুতকারকের যন্ত্রে ২২টি অজানা দুর্বলতা আবিষ্কার করেছি এবং কার্যকর এক্সপ্লয়েটে আক্রমণ দেখিয়েছি: ECG অ্যালার্ম বন্ধ করা, জীবাণুমুক্ত অপারেশন কক্ষের বায়ু চলাচল থামানো এবং রক্তের গ্রুপ ও অ্যালার্জির তথ্য বদলানো। নিজস্ব SOP/CORS বাইপাস দিয়ে ইন্টারনেট থেকে সরাসরি প্রবেশযোগ্য নয় এমন অভ্যন্তরীণ যন্ত্রেও দূরবর্তী আক্রমণ দেখিয়েছি।

পরীক্ষিত প্রস্তুতকারকদের মধ্যে ZEISS, MOXA, Zebra, Dedalus Labor ও Tetronik রয়েছে। Golem-এর ২০২৪ সালের প্রতিবেদন অনুযায়ী যন্ত্রগুলো আরও হাজার হাজার হাসপাতাল ও চিকিৎসাকেন্দ্রে ব্যবহৃত হতো। আমি প্রস্তুতকারকদের জানানো ও সমাধানে সহায়তার সমন্বয় করেছি। প্রস্তুতকারকদের জানানো থেকে সমাধানে আমার সহায়তা পর্যন্ত পুরো প্রক্রিয়া সাংবাদিকরা অনুসরণ করেছেন।

৪০টির বেশি সরকারি সংস্থা, **OBI**, **REWE** ও **Fraunhofer** ইনস্টিটিউটে নিরাপত্তার দুর্বলতা

৪৫টি পৌর প্রশাসন ও কোম্পানিতে দুর্বলতা আবিষ্কার করে দায়িত্বশীলদের জানিয়েছি। OBI-তে একটি ওয়েব দুর্বলতায় ব্যবহারকারীর সেশন দখল ও অভ্যন্তরীণ কনটেন্ট ব্যবস্থাপনা থেকে তথ্য পড়া সম্ভব ছিল।

অনেক পৌরসভা ত্রুটি সংশোধন করেছে। প্রকাশ্য বিতর্কের পর OBI সংশ্লিষ্ট সাইট বন্ধ করে। Golem ও WirtschaftsWoche গবেষণা এবং কোম্পানিগুলোর প্রতিক্রিয়া নথিবদ্ধ করেছে।

অভিজ্ঞতা

জুন ২০২৩ - বর্তমান

CEO · CTO · CYTRES GmbH
সফটওয়্যার উন্নয়ন ও সাইবার নিরাপত্তা গবেষণায় গুরুত্ব দিয়ে প্রতিষ্ঠানটি প্রতিষ্ঠা ও পরিচালনা করেছি।

ডিসে ২০১৬ - আগ ২০১৯

সাইবার নিরাপত্তা টিউটর · CIC (Cambridge Innovation Center) · Rotterdam, নেদারল্যান্ডস
সাইবার নিরাপত্তা কর্মশালা ও কারিগরি প্রশিক্ষণ পরিচালনা করেছি।

ডিসে ২০১৬ - আগ ২০১৯

সিনিয়র নিরাপত্তা উপদেষ্টা · Base Cyber Security · Rotterdam, নেদারল্যান্ডস
কারিগরি দলের নেতৃত্ব দিয়েছি এবং নতুন কর্মীদের প্রয়োজনীয় কারিগরি মান পর্যন্ত প্রশিক্ষণ দিয়েছি।

2019

প্রতিষ্ঠাতা · **CEO** · **CTO** · Secbiz IT Security GmbH
- সাইবার নিরাপত্তা প্রতিষ্ঠানের প্রতিষ্ঠাতা ও প্রযুক্তি প্রধান।
- শিল্প/OT ও অ্যাপ নিরাপত্তায় গবেষণা এবং পরামর্শ।

- Hannover Messe 2019-এ SCADA আক্রমণের সরাসরি প্রদর্শনী।

Veloce

Veloce হলো agentic coding-এর জন্য আমার JavaScript/TypeScript runtime: এমন একটি target platform যেখানে coding agent-রা সম্পূর্ণ application তৈরি করতে পারে যা পড়া যায়, audit করা যায় এবং সরাসরি চালানো যায় - আগে npm dependency, framework, build tooling ও deployment glue জোড়া লাগানো ছাড়াই।

Runtime গুরুত্বপূর্ণ building block-গুলো সরাসরি দেয়: সীমাবদ্ধ sandbox ও permission model, HTTP server, ORM ও KV store-সহ SQLite/PostgreSQL, browser ও desktop capability এবং standalone native binary-তে packaging। ভারী computation JavaScript/TypeScript থেকে Rust-backed native kernel বা WebAssembly-তে offload করা যায়। লক্ষ্য হলো এমন software যা agent-রা নির্ভরযোগ্যভাবে তৈরি করতে পারে, মানুষ বুঝতে পারে এবং system খুব কম moving part নিয়ে চালাতে পারে।

দক্ষতা

Embedded, OT ও medical device

Firmware ও connected device-এ vulnerability research: fire alarm system, industrial controller (SCADA), hospital ও medical equipment।

Exploit development

একটি memory-corruption bug থেকে remote root access-সহ পূর্ণ exploit chain পর্যন্ত।

Browser ও web security

SOP/CORS bypass, internal network device-এ attack path, XSS এবং application security।

Responsible disclosure

Vendor ও operator-দের সঙ্গে reporting এবং coordination, বড় কোম্পানি থেকে municipal administration পর্যন্ত, remediation support-সহ।

নিজস্ব **tools**

Vulnerability discovery ও penetration testing-এর জন্য tooling এবং automation, AI-assisted workflow-সহ। Veloce JavaScript/TypeScript runtime-এর নির্মাতা।

গবেষণা

বছর	গবেষণা / দুর্বলতা	উৎস
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	CIRCL-এ CISA এন্ট্রি
2013	Apple Motion - CVE-2013-6114 - নিরাপত্তা দুর্বলতা	Apple
2014	Apple Web Server - নিরাপত্তা গবেষণা, ফেব্রুয়ারি ২০১৪	Apple
2012	Nokia Hall of Fame - নিরাপত্তা গবেষণা, ডিসেম্বর ২০১২	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit মডিউল	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq আর্কাইভ
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

সংবাদমাধ্যম

বছর	মূল প্রতিবেদন	মাধ্যম
2025	Securitas / Marvelit-এ দায়িত্বশীল প্রকাশ নিয়ে প্রতিবেদন	Security-Insider
2022	সাইবার নিরাপত্তা ও নৈতিক হ্যাকিং নিয়ে রেডিও অনুষ্ঠান	WDR
2024	ÖAG বিশেষজ্ঞ আলোচনা: নিরাপত্তা 4.0 - সাইবার নিরাপত্তা ও AI-ভিত্তিক প্রতিরক্ষা	medianet (অস্ট্রিয়া)
2024	হাসপাতালে নিরাপত্তা দুর্বলতা: রোগীরা ঝুঁকিতে	Golem
2024	ব্রাউজার SOP/CORS ও অভ্যন্তরীণ নেটওয়ার্ক ডিভাইস	CYTRES Research
2024	Jean Pereira-এর জনসম্মুখের নিরাপত্তা বিজ্ঞপ্তি, সমাধান সম্পর্কে নথিবদ্ধ আপডেটসহ	Volksbank / Sparda Bank (Responsible Disclosure)
2023	রাষ্ট্রসচিব টুরস্কির সঙ্গে ডিজিটালাইজেশন, AI ও সাইবার নিরাপত্তা নিয়ে বিশেষজ্ঞ আলোচনা	KURIER (অস্ট্রিয়া)
2023	ÖAG Super Tuesday-তে সাইবার নিরাপত্তা বিশেষজ্ঞ হিসেবে অংশগ্রহণ	LEADERSNET (অস্ট্রিয়া)
2022	পডকাস্ট #51: Ethical Hacker - নিরাপত্তা গবেষণা ও পেশাগত পথ	IDG TechTalk / COMPUTERWOCHE
2022	কোলন শহর প্রশাসনে IT নিরাপত্তা দুর্বলতা	Kölner Stadt-Anzeiger
2022	জানানো নিরাপত্তা দুর্বলতা উপেক্ষা করায় তথ্য সুরক্ষা কমিশনার তদন্ত করছেন	WirtschaftsWoche
2022	দায়িত্বশীল প্রকাশ / ৪৫টি সংস্থা	Golem
2022	OBI ও সরকারি কর্তৃপক্ষ নিয়ে প্রতিবেদন	connect professional
2020	ব্রাউজার ও অ্যাপ্লিকেশন নিরাপত্তা নিয়ে মূল বক্তব্য	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: লাইভ SCADA/ICS হ্যাকিং	Hannover Messe / MittelstandsWiki
2019	সাক্ষাৎকার "আমাদের আরও হ্যাকার দরকার"	atp magazin
2019	সাইবার আক্রমণ ও ডার্কনেট - Jean Pereira-এর সাক্ষাৎকার	Podcast "IT'S IN YOU"
2018	SEO-DAY: ২০১৮ সালে Chrome হ্যাক ও SSL বাইপাস করার উপায়	Host Europe
2018	SEO-DAY 2018-এর সুপারপ্যানেলে নিরাপত্তা বক্তৃতা	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker ও SECBIZ প্রতিষ্ঠাতা বক্তাদের তালিকায়	DSS IT SEC / Riga