Jean Pereira

Sicherheitsforschung · Offensive Security · Full-Stack-Entwicklung

Ich untersuche komplexe Systeme auf Sicherheitslücken und entwickle Sicherheitssoftware und eigene Produkte. Meine Arbeit umfasst Browser- und Embedded-Security, industrielle Systeme, Automatisierung und KI.

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

Profil

Ich finde Sicherheitslücken dort, wo andere aufhören zu suchen, und baue sichere Software, die komplexe Probleme löst.

Zu meinen Arbeiten gehören Schwachstellen in Produkten und Technologien von **Siemens**, **Apple**, **Google**, **Microsoft** und **Nokia** sowie diversen Projekten in der Medizintechnik. Aktuell liegt mein Fokus auf Security Research und Software Engineering.

Außerdem bin ich Autor von **Veloce**. Du erreichst mich über das Kontaktformular oder direkt auf LinkedIn.

Highlights

Vier Zero-Days bei Siemens: Alarmsysteme und Brandmelder aus der Ferne übernommen

Ich habe Alarmsysteme und Brandmelder von Siemens aus der Ferne vollständig übernommen. Mein selbst entwickelter Exploit verschaffte mir die höchsten Systemrechte auf den Geräten. Dafür waren weder Zugangsdaten noch ein Klick oder eine andere Mitwirkung des Nutzers nötig.

Ich entdeckte vier zuvor unbekannte Sicherheitslücken und kombinierte sie zu einer funktionierenden Angriffskette. Mit den erlangten Root-Rechten konnte ich eigenen Code auf Betriebssystemebene ausführen und die Geräte vollständig kontrollieren. Diese Übernahme habe ich praktisch nachgewiesen.

Siemens bestätigte meine Forschung in einem eigenen Security-Advisory. Der Exploit erhielt CVSS 10.0, die maximal mögliche Kritikalität. Die vier Funde sind als CVE-2024-47901, CVE-2024-47902, CVE-2024-47903 und CVE-2024-47904 dokumentiert.

Zero-Days in Krankenhäusern: Blutgruppen manipuliert, EKG-Alarme und Belüftungsgeräte abgeschaltet

Bei einer Sicherheitsanalyse entdeckte ich 22 zuvor unbekannte Schwachstellen in Geräten von zwölf Herstellern und wies die Angriffe mit funktionierenden Exploits praktisch nach: EKG-Alarme abschalten, die Belüftung steriler OP-Säle unterbrechen sowie Blutgruppen und Allergieinformationen manipulieren. Mit eigens entwickelten SOP/CORS-Bypasses demonstrierte ich außerdem Fernangriffe auf interne Geräte, die selbst nicht aus dem Internet erreichbar waren.

Zu den untersuchten Herstellern gehören ZEISS, MOXA, Zebra, Dedalus Labor und Tetronik. Laut Golems Reportage von 2024 waren die betroffenen Geräte in Tausenden weiteren Krankenhäusern und medizinischen Einrichtungen im Einsatz. Ich koordinierte die Offenlegung an die Hersteller und begleitete die Behebung. Journalisten begleiteten den gesamten Prozess, von der Meldung an die Hersteller bis zu meiner Unterstützung bei der Behebung.

Sicherheitslücken bei über 40 Behörden, OBI, REWE und dem Fraunhofer-Institut

Ich deckte Sicherheitslücken bei insgesamt 45 Stadtverwaltungen und Unternehmen auf und meldete sie den Verantwortlichen. Bei OBI ging es um eine Web-Schwachstelle, über die sich Nutzersitzungen übernehmen und Informationen aus dem internen Redaktionssystem auslesen ließen.

Viele der betroffenen Stadtverwaltungen schlossen die gemeldeten Lücken. OBI nahm die betroffene Website nach der öffentlichen Auseinandersetzung vom Netz. Golem und WirtschaftsWoche dokumentierten die Recherche und den Umgang der Unternehmen mit den Funden.

Erfahrung

Jun. 2023 - heute

CEO · CTO · CYTRES GmbH
Gründung und Leitung mit Schwerpunkt auf Softwareentwicklung und Sicherheitsforschung.

Dez. 2016 - Aug. 2019

Tutor für Cybersecurity · CIC (Cambridge Innovation Center) · Rotterdam, Südholland, Niederlande
Durchführung von Cybersecurity-Workshops und technischen Schulungen.

Dez. 2016 - Aug. 2019

Senior Security Advisor · Base Cyber Security · Rotterdam, Südholland, Niederlande
Verantwortung für das technische Team sowie Einarbeitung und Training neuer Mitarbeiter bis zum erforderlichen technischen Standard.

2019

Gründer · CEO · CTO · Secbiz IT Security GmbH

- Gründung und technische Leitung eines Security-Unternehmens; Sicherheitsforschung, Beratung und Penetration Testing.
- Schwerpunkt Industrie-/OT-Security, Web- und Application Security sowie Schwachstellenanalyse.
- Vortrag und Live-Demonstration auf der Hannover Messe 2019 zum Angriff auf industrielle SCADA-Steuerungen.

Veloce

Veloce ist meine JavaScript/TypeScript-Runtime für Agentic Coding: eine Zielplattform, auf der Coding-Agents vollständige Anwendungen erzeugen können, die lesbar, nachvollziehbar und direkt ausführbar sind, ohne zuerst npm-Abhängigkeiten, Frameworks, Build-Tooling und Deployment-Glue zusammenzustecken.

Die Runtime bringt dafür die entscheidenden Bausteine direkt mit: ein restriktives Sandbox- und Permission-Modell, HTTP-Server, SQLite und PostgreSQL samt ORM und KV-Store, Browser- und Desktop-Funktionen sowie Packaging zu einer eigenständigen nativen Binary. Rechenintensive Pfade lassen sich aus JavaScript/TypeScript an Rust-basierte native Kernels oder WebAssembly auslagern. Das Ziel ist Software, die Agents zuverlässig erzeugen können, Menschen weiterhin verstehen und Systeme mit möglichst wenigen beweglichen Teilen ausführen können.

Expertise

Embedded, OT & Medizintechnik

Schwachstellenforschung in Firmware und vernetzten Geräten: Brandmeldetechnik, Industriesteuerungen (SCADA), Krankenhaus- und Medizingeräte.

Exploit-Entwicklung

Vom einzelnen Memory-Corruption-Fund bis zur Exploit-Chain mit Remote-Root-Zugriff.

Browser- & Web-Sicherheit

SOP/CORS-Bypässe, Angriffspfade auf Geräte im internen Netzwerk, XSS und Anwendungssicherheit.

Responsible Disclosure

Meldung und Abstimmung mit Herstellern und Betreibern, von Konzernen bis zu Stadtverwaltungen, einschließlich Unterstützung bei der Behebung.

Eigene Werkzeuge

Tooling und Automatisierung für Schwachstellensuche und Pentesting, auch mit KI-Unterstützung. Autor der JavaScript/TypeScript-Runtime Veloce.

Forschung

Jahr	Forschung / Schwachstelle	Quelle
2024	Siemens ProductCERT, SSA-333468 - CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904; Remote Code Execution als root	Siemens
2024	Siemens InterMesh - CISA ICS-Advisory ICSA-24-303-01	CISA-Eintrag bei CIRCL
2013	Apple Motion - CVE-2013-6114 - Sicherheitslücke in Apple Motion	Apple
2014	Apple Web Server - Security Research, Februar 2014	Apple
2012	Nokia Hall of Fame - Security Research, Dezember 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit-Modul	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq-Archiv
2012	PhpTax - CVE-2012-10037 - Remote Command Injection	OpenCVE

Jahr	Forschung / Schwachstelle	Quelle
2012	b2ePMS - CVE-2012-6626 - SQL Injection / Authentication Bypass	Bugtraq
2012	HCView Remote Code Execution - BID 55819	Bugtraq
2012	DomsHttpd Remote DoS - 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

Presse

Jahr	Originalbericht	Medium
2025	Berichterstattung zu Responsible Disclosure bei Securitas / Marvelit	Security-Insider
2022	Radiobeitrag zu Cybersecurity und Ethical Hacking	WDR
2024	ÖAG-Expertentalk: Sicherheit 4.0 - Cybersecurity und KI-Abwehr	medianet (Österreich)
2024	Sicherheitslücken in Krankenhäusern: Patienten in Gefahr	Golem
2024	Browser SOP/CORS und interne Netzwerkgeräte	CYTRES Research
2024	Öffentliche Sicherheitsmeldung von Jean Pereira mit dokumentiertem Behebungs-Update	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Expertentalk mit Staatssekretär Tursky über Digitalisierung, KI und Cybersecurity	KURIER (Österreich)
2023	Als Cybersecurity-Experte beim ÖAG Super Tuesday zugeschaltet	LEADERSNET (Österreich)
2022	Podcast #51: Ethical Hacker - Sicherheitsforschung und Werdegang	IDG TechTalk / COMPUTERWOCHE
2022	IT-Sicherheitslücke bei der Stadt Köln	Kölner Stadt-Anzeiger
2022	Wegen ignorierter gemeldeter Sicherheitslücke ermittelt die Datenschutzbeauftragte	WirtschaftsWoche
2022	Responsible Disclosure / 45 Organisationen	Golem
2022	Bericht zu OBI und Behörden	connect professional
2020	Keynote zur Browser- und Anwendungssicherheit	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: Live SCADA/ICS Hacking	Hannover Messe / MittelstandsWiki
2019	Interview "Wir brauchen mehr Hacker"	atp magazin
2019	Cyberangriffe & Darknet - Jean Pereira im Interview	Podcast "IT'S IN YOU"
2018	SEO-DAY: How to hack Chrome and bypass SSL in 2018	Host Europe
2018	Security-Vortrag im Superpanel des SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker und SECBIZ-Gründer im Speaker-Line-up	DSS IT SEC / Riga