Jean Pereira

資安研究 · 攻防安全 · 全端工程

我研究複雜系統中的漏洞，並在瀏覽器安全、嵌入式與工業系統、自動化和人工智慧等領域開發安全軟體與自己的產品。

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

個人簡介

我在他人停止尋找的地方發現安全弱點，並開發解決複雜問題的安全軟體。

我的工作包括 **Siemens**、**Apple**、**Google**、**Microsoft** 和 **Nokia** 的產品與技術中的漏洞，以及醫療技術領域的各種專案。目前我專注於資安研究和軟體工程。

我也是 **Veloce** 的作者。你可以透過聯絡表單或直接在 LinkedIn 上聯絡我。

重點

Siemens 的四項零時差漏洞：遠端接管警報系統與火災探測器

我遠端完全接管了 Siemens 警報系統與火災探測器。我的漏洞利用取得 root 存取權，也就是裝置上的最高系統權限，不需要登入憑證、點擊或受害者的任何配合。

我開發了串聯四項未知弱點的利用鏈，並實際展示完整接管。這代表掌控攸關安全的警報技術。

Siemens 確認了這四項發現，編號為 CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904。此漏洞利用獲評 CVSS 10.0，即可能的最高嚴重程度。

醫院零時差漏洞：血型遭竄改，心電警報與通風設備遭關閉

在一次安全評估中，我發現十二家廠商裝置中的 22 項未知弱點，並以可運作的漏洞利用展示攻擊：關閉心電監測警報、中斷無菌手術室通風，以及竄改血型和過敏紀錄。我也開發了 SOP/CORS 繞過方法，展示對無法從網際網路直接存取的內部裝置進行遠端攻擊。

研究涉及 ZEISS、MOXA、Zebra、Dedalus Labor 和 Tetronik 等廠商。依據 Golem 2024 年報導，相關裝置亦部署於數千家其他醫院及醫療機構。我協調向廠商揭露弱點，並協助修補。 記者跟進整個過程，從向廠商通報弱點，到我協助廠商進行修補。

40 多家政府機構、OBI、REWE 及弗勞恩霍夫研究所的安全弱點

我在 45 家市政機構與企業發現安全弱點，並向負責人通報。在 OBI，一項網頁弱點可用來劫持使用者工作階段及讀取內部內容管理系統的資訊。

許多市政機構修補了問題。公開爭議後，OBI 關閉相關網站。Golem 與 WirtschaftsWoche 記錄了研究及企業處理發現的方式。

工作經歷

2023 年 6 月 - 至今

CEO · CTO · CYTRES GmbH
創立並領導公司，重點投入軟體開發與資安研究。

2016 年 12 月 - 2019 年 8 月

資安導師 · CIC (Cambridge Innovation Center) · Rotterdam, 荷蘭
舉辦資安工作坊與技術培訓。

2016 年 12 月 - 2019 年 8 月

資深資安顧問 · Base Cyber Security · Rotterdam, 荷蘭
帶領技術團隊，並將新進員工培訓至所需的技術水準。

2019

創辦人 · CEO · CTO · Secbiz IT Security GmbH

- 資安公司的創辦人與技術負責人。
- 從事工業 / OT 安全、應用安全研究與顧問工作。
- 2019 年在 Hannover Messe 現場示範 SCADA 系統攻擊。

Veloce

Veloce 是我為 agentic coding 開發的 JavaScript/TypeScript 執行環境：一個面向程式代理的目標平台，讓 agent 可以產生完整、可讀、可稽核且能直接執行的應用程式，而不必先拼裝 npm 相依套件、framework、build 工具與 deployment glue。

執行環境直接提供關鍵能力：受限的 sandbox 與權限模型、HTTP 服務、含 ORM 與 KV 儲存的 SQLite/PostgreSQL、瀏覽器與桌面功能，以及封裝成獨立原生二進位檔。計算密集的路徑可由 JavaScript/TypeScript 下沉到 Rust-backed native kernel 或 WebAssembly。目標是讓 agent 能可靠產生、開發者仍能理解、系統能以盡可能少的活動元件執行的軟體。

專業技能

嵌入式、OT 與醫療設備

針對韌體和連網裝置的漏洞研究：火災警報系統、工業控制器（SCADA）、醫院和醫療設備。

漏洞利用開發

從單一記憶體破壞漏洞到可取得遠端 root 權限的完整利用鏈。

瀏覽器與 Web 安全

SOP/CORS 繞過、針對內部網路裝置的攻擊路徑、XSS 與應用程式安全。

負責任揭露

與廠商和營運方進行通報與協調，範圍從大型企業到市政機關，並協助完成修復。

自研工具

用於漏洞發現和滲透測試的工具與自動化，包括 AI 輔助工作流程。Veloce JavaScript/TypeScript runtime 的作者。

研究

年份	研究 / 漏洞	來源
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 上的 CISA 項目
2013	Apple Motion - CVE-2013-6114 - 資安漏洞	Apple
2014	Apple Web Server - 資安研究, 2014 年 2 月	Apple
2012	Nokia Hall of Fame - 資安研究, 2012 年 12 月	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit 模組	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq 封存
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

媒體報導

年份	原文	媒體
2025	Securitas / Marvelit 負責任揭露事件報導	Security-Insider

年份	原文	媒體
2022	關於網路安全與道德駭客的廣播節目	WDR
2024	ÖAG 專家對談：安全 4.0 - 網路安全與 AI 防禦	medianet (奧地利)
2024	醫院安全漏洞：病患面臨風險	Golem
2024	瀏覽器 SOP/CORS 與內部網路裝置	CYTRES Research
2024	Jean Pereira 發布的公開資安通報及有紀錄的修復更新	Volksbank / Sparda Bank (Responsible Disclosure)
2023	與國務秘書 Tursky 就數位化、AI 與網路安全進行專家對談	KURIER (奧地利)
2023	以資安專家身分參與 ÖAG Super Tuesday	LEADERSNET (奧地利)
2022	Podcast #51：Ethical Hacker - 資安研究與職涯歷程	IDG TechTalk / COMPUTERWOCHE
2022	科隆市政府的 IT 資安漏洞	Kölner Stadt-Anzeiger
2022	已通報的安全漏洞遭忽視，資料保護專員展開調查	WirtschaftsWoche
2022	負責任揭露 / 45 個組織	Golem
2022	關於 OBI 與公部門的報導	connect professional
2020	關於瀏覽器與應用程式安全的主題演講	OMT - Online Marketing Konferenz
2019	Industrial Security Forum：現場 SCADA/ICS 駭客展示	Hannover Messe / MittelstandsWiki
2019	訪談《我們需要更多駭客》	atp magazin
2019	網路攻擊與暗網 - Jean Pereira 訪談	Podcast "IT'S IN YOU"
2018	SEO-DAY：2018 年如何入侵 Chrome 並繞過 SSL	Host Europe
2018	SEO-DAY 2018 超級論壇中的安全演講	SEO-DAY / Online-Profession
2018	International Cyber Security Conference：Ethical Hacker 與 SECBIZ 創辦人進入講者陣容	DSS IT SEC / Riga