Jean Pereira

安全研究 · 攻防安全 · 全栈工程

我研究复杂系统中的漏洞，并在浏览器安全、嵌入式和工业系统、自动化及人工智能等领域开发安全软件和自己的产品。

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

个人简介

我在他人停止寻找的地方发现安全漏洞，并开发解决复杂问题的安全软件。

我的工作包括 **Siemens**、**Apple**、**Google**、**Microsoft** 和 **Nokia** 的产品与技术中的漏洞，以及医疗技术领域的各种项目。目前我专注于安全研究和软件工程。

我也是 **Veloce** 的作者。你可以通过联系表单或直接在 LinkedIn 上联系我。

亮点

Siemens 的四项零日漏洞：远程接管报警系统与火灾探测器

我远程完全接管了 Siemens 报警系统与火灾探测器。我的漏洞利用获得了 root 访问权限，也就是设备上的最高系统权限，不需要登录凭据、点击或受害者的任何配合。

我开发了串联四项未知漏洞的利用链，并在实践中演示了完整接管。这意味着掌控对安全至关重要的报警技术。

Siemens 确认了这四项发现，编号为 CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904。该漏洞利用获评 CVSS 10.0，即可能的最高严重程度。

医院零日漏洞：血型已被篡改，心电报警与通风设备已被关闭

在一次安全评估中，我发现了十二家厂商设备中的 22 项未知漏洞，并以可运行的漏洞利用演示了攻击：关闭心电监护报警、中断无菌手术室通风，以及篡改血型和过敏记录。我还开发了 SOP/CORS 绕过方法，演示了对无法从互联网直接访问的内部设备实施远程攻击。

研究涉及 ZEISS、MOXA、Zebra、Dedalus Labor 和 Tetronik 等厂商。据 Golem 2024 年的报道，相关设备也部署在数千家其他医院及医疗机构。我协调了向厂商的漏洞披露，并协助修复。 记者跟进了整个过程，从向厂商报告漏洞，到我协助厂商开展修复。

40 多家政府机构、OBI、REWE 及弗劳恩霍夫研究所的安全漏洞

我在 45 家市政机构和企业中发现安全漏洞，并向负责人报告。在 OBI，一项网页漏洞可用于劫持用户会话和读取内部内容管理系统的信息。

许多市政机构修复了所报告的问题。公开争议后，OBI 下线了相关网站。Golem 和 WirtschaftsWoche 记录了研究及企业对发现的处理方式。

工作经历

2023 年 6 月 - 至今

CEO · CTO · CYTRES GmbH
创立并领导公司，重点从事软件开发和网络安全研究。

2016 年 12 月 - 2019 年 8 月

网络安全导师 · CIC (Cambridge Innovation Center) · Rotterdam, 荷兰
开展网络安全研讨会和技术培训。

2016 年 12 月 - 2019 年 8 月

高级安全顾问 · Base Cyber Security · Rotterdam, 荷兰
负责技术团队，并将新员工培训至所需的技术水平。

2019

创始人 · CEO · CTO · Secbiz IT Security GmbH

- 网络安全公司的创始人及技术负责人。
- 从事工业/OT 安全、应用安全研究与咨询。
- 2019 年在 Hannover Messe 现场演示 SCADA 系统攻击。

Veloce

Veloce 是我为 agentic coding 开发的 JavaScript/TypeScript 运行时：一个面向编码智能体的目标平台，让智能体可以生成完整、可读、可审计并能直接运行的应用，而不必先拼装 npm 依赖、框架、构建工具和部署胶水。

运行时直接提供关键能力：受限的 sandbox 与权限模型、HTTP 服务、带 ORM 和 KV 存储的 SQLite/PostgreSQL、浏览器与桌面能力，以及打包为独立原生二进制文件。计算密集型路径可以从 JavaScript/TypeScript 下沉到基于 Rust 的原生 kernel 或 WebAssembly。目标是让智能体能够可靠生成、开发者仍能理解、系统能够以尽可能少的活动部件运行的软件。

专业技能

嵌入式、OT 与医疗设备

针对固件和联网设备的漏洞研究：火灾报警系统、工业控制器（SCADA）、医院和医疗设备。

漏洞利用开发

从单个内存破坏漏洞到可获得远程 root 权限的完整利用链。

浏览器与 Web 安全

SOP/CORS 绕过、针对内部网络设备的攻击路径、XSS 和应用安全。

负责任披露

与厂商和运营方进行报告和协调，范围从大型企业到市政机构，并协助完成修复。

自研工具

用于漏洞发现和渗透测试的工具与自动化，包括 AI 辅助工作流。Veloce JavaScript/TypeScript runtime 的作者。

研究

年份	研究 / 漏洞	来源
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 条目
2013	Apple Motion - CVE-2013-6114 - 安全漏洞	Apple
2014	Apple Web Server - 安全研究, 2014 年 2 月	Apple
2012	Nokia Hall of Fame - 安全研究, 2012 年 12 月	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit 模块	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq 存档
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

媒体报道

年份	原文	媒体
2025	Securitas / Marvelit 负责任披露事件报道	Security-Insider
2022	关于网络安全与道德黑客的广播节目	WDR

年份	原文	媒体
2024	ÖAG 专家对谈：安全 4.0 - 网络安全与 AI 防御	medianet (奥地利)
2024	医院安全漏洞：患者面临风险	Golem
2024	浏览器 SOP/CORS 与内部网络设备	CYTRES Research
2024	Jean Pereira 发布的公开安全通告及有记录的修复更新	Volksbank / Sparda Bank (Responsible Disclosure)
2023	与国务秘书 Tursky 就数字化、AI 与网络安全进行专家对谈	KURIER (奥地利)
2023	以网络安全专家身份参加 ÖAG Super Tuesday	LEADERSNET (奥地利)
2022	播客 #51：Ethical Hacker - 安全研究与职业历程	IDG TechTalk / COMPUTERWOCHE
2022	科隆市政府的 IT 安全漏洞	Kölner Stadt-Anzeiger
2022	已报告的安全漏洞遭忽视，数据保护专员展开调查	WirtschaftsWoche
2022	负责任披露 / 45 家组织	Golem
2022	关于 OBI 与公共机构的报道	connect professional
2020	关于浏览器与应用安全的主题演讲	OMT - Online Marketing Konferenz
2019	Industrial Security Forum：现场 SCADA/ICS 黑客演示	Hannover Messe / MittelstandsWiki
2019	访谈《我们需要更多黑客》	atp magazin
2019	网络攻击与暗网 - Jean Pereira 访谈	Podcast "IT'S IN YOU"
2018	SEO-DAY：2018 年如何入侵 Chrome 并绕过 SSL	Host Europe
2018	SEO-DAY 2018 超级论坛中的安全演讲	SEO-DAY / Online-Profession
2018	International Cyber Security Conference：Ethical Hacker 与 SECBIZ 创始人进入演讲嘉宾阵容	DSS IT SEC / Riga