Jean Pereira

セキュリティ研究 · Offensive Security · フルスタック開発

複雑なシステムの脆弱性を研究し、ブラウザセキュリティ、組み込みおよび産業システム、自動化、AI の分野でセキュリティソフトウェアと独自製品を開発しています。

Jean Pascal José Pereira · ドイツ · LinkedIn · pereira.cv/contact

---

プロフィール

他の人が探すのをやめた先でセキュリティの脆弱性を見つけ、複雑な問題を解決する安全なソフトウェアを作ります。

これまでの仕事には **Siemens**、**Apple**、**Google**、**Microsoft**、**Nokia** の製品や技術の脆弱性、および 医療技術分野のさまざまなプロジェクトが含まれます。現在はセキュリティ研究とソフトウェアエンジニアリングに注力しています。

また、**Veloce** の作者でもあります。お問い合わせフォーム、または LinkedIn から直接ご連絡いただけます。

ハイライト

Siemens の 4 件のゼロデイ：警報システムと火災感知器を遠隔から掌握

Siemens の警報システムと火災感知器を、遠隔から完全に掌握しました。私のエクスプロイトは機器上で最高のシステム権限である root アクセスを取得しました。認証情報もクリックも、被害者の操作も不要でした。

4 件の未知の脆弱性を組み合わせたエクスプロイトチェーンを開発し、完全な乗っ取りを実証しました。安全に直結する警報技術の制御を奪う結果です。

Siemens は 4 件の発見を CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904 として確認しました。エクスプロイトは CVSS 10.0 と評価され、最大の深刻度を示します。

病院のゼロデイ：血液型を改ざん、心電図アラームと換気装置を停止

セキュリティ評価で 12 社の機器に 22 件の未知の脆弱性を発見し、動作するエクスプロイトで攻撃を実証しました。心電図アラームの停止、無菌手術室の換気停止、血液型・アレルギー情報の改ざんが含まれます。独自の SOP/CORS 回避手法を開発し、インターネットから直接接続できない内部機器への遠隔攻撃も実証しました。

調査対象には ZEISS、MOXA、Zebra、Dedalus Labor、Tetronik が含まれます。Golem の 2024 年の報道によると、該当機器は他の数千の病院・医療施設でも使用されていました。メーカーへの開示を調整し、修正を支援しました。メーカーへの報告から修正支援まで、一連の過程をジャーナリストが取材しました。

40 を超える行政機関、OBI、REWE、フラウンホーファー研究所の脆弱性

45 の自治体・企業で脆弱性を発見し、担当者に報告しました。OBI のウェブ脆弱性は、ユーザーセッションの乗っ取りや内部コンテンツ管理システムの情報取得を可能にするものでした。

多くの自治体は問題を修正しました。OBI は公開の議論後、該当サイトを停止しました。Golem と WirtschaftsWoche は研究と企業の対応を報道しました。

経歴

2023 年 6 月 - 現在

CEO · CTO · CYTRES GmbH
ソフトウェア開発とサイバーセキュリティ研究を中心に会社を設立・経営しました。

2016 年 12 月 - 2019 年 8 月

サイバーセキュリティ講師 · CIC (Cambridge Innovation Center) · Rotterdam, オランダ
サイバーセキュリティのワークショップと技術研修を実施しました。

2016 年 12 月 - 2019 年 8 月

シニアセキュリティアドバイザー · Base Cyber Security · Rotterdam, オランダ
技術チームを率い、新入社員を必要な技術水準まで育成しました。

2019

創業者 · CEO · CTO · Secbiz IT Security GmbH

- サイバーセキュリティ企業の創業者・技術責任者。
- 産業制御 / OT セキュリティとアプリケーションセキュリティの研究・コンサルティング。
- Hannover Messe 2019 で SCADA 侵入のライブデモを実施。

Veloce

Veloce は agentic coding のために私が開発している JavaScript/TypeScript ランタイムです。コーディングエージェントが npm 依存関係、フレームワーク、ビルドツール、デプロイ用の glue を先に組み合わせることなく、読みやすく監査可能で、そのまま実行できる完全なアプリケーションを生成するためのターゲットプラットフォームです。

ランタイムには重要な構成要素が最初から統合されています。制限的な sandbox と権限モデル、HTTP サーバー、ORM と KV ストアを備えた SQLite/PostgreSQL、ブラウザ / デスクトップ機能、そして単体のネイティブバイナリへのパッケージングです。計算負荷の高い処理は JavaScript/TypeScript から Rust ベースのネイティブ kernel や WebAssembly に移せます。エージェントが安定して生成でき、人間が理解でき、システムが最小限の可動部で実行できるソフトウェアを目指しています。

専門分野

組み込み、OT、医療機器

ファームウェアと接続機器の脆弱性研究。火災報知システム、産業用コントローラ（SCADA）、病院・医療機器を対象としています。

Exploit 開発

単一の memory corruption バグから、リモート root アクセスを実現する完全な exploit chain まで。

ブラウザと Web セキュリティ

SOP/CORS バイパス、内部ネットワーク機器への攻撃経路、XSS、アプリケーションセキュリティ。

責任ある開示

大企業から自治体まで、ベンダーや運用者への報告と調整を行い、修正作業も支援します。

独自ツール

脆弱性発見と penetration testing のためのツールと自動化、AI 支援 workflow を含みます。JavaScript/TypeScript runtime Veloce の作者です。

研究

年	研究 / 脆弱性	出典
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 の CISA エントリ
2013	Apple Motion - CVE-2013-6114 - 脆弱性	Apple
2014	Apple Web Server - セキュリティ研究, 2014 年 2 月	Apple
2012	Nokia Hall of Fame - セキュリティ研究, 2012 年 12 月	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit モジュール	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq アーカイブ
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

メディア

年	元の記事	媒体
2025	Securitas / Marvelit における責任ある開示に関する報道	Security-Insider
2022	サイバーセキュリティとエシカルハッキングに関するラジオ番組	WDR
2024	ÖAG 専門家トーク：セキュリティ 4.0 - サイバーセキュリティと AI 防御	medianet (オーストリア)
2024	病院のセキュリティ脆弱性：患者が危険にさらされる	Golem
2024	ブラウザの SOP/CORS と内部ネットワーク機器	CYTRES Research
2024	Jean Pereira による公開セキュリティ通知と修正状況の記録付きアップデート	Volksbank / Sparda Bank (Responsible Disclosure)
2023	トゥルスキー国務次官とデジタル化、AI、サイバーセキュリティを語る専門家トーク	KURIER (オーストリア)
2023	ÖAG Super Tuesday にサイバーセキュリティ専門家として参加	LEADERSNET (オーストリア)
2022	ポッドキャスト #51：Ethical Hacker - セキュリティ研究とキャリア	IDG TechTalk / COMPUTERWOCHE
2022	ケルン市の IT セキュリティ脆弱性	Kölner Stadt-Anzeiger
2022	報告されたセキュリティ脆弱性の放置を受け、データ保護委員が調査	WirtschaftsWoche
2022	責任ある開示 / 45 組織	Golem
2022	OBI と行政機関に関する報道	connect professional
2020	ブラウザおよびアプリケーションセキュリティに関する基調講演	OMT - Online Marketing Konferenz
2019	Industrial Security Forum：SCADA/ICS ライブハッキング	Hannover Messe / MittelstandsWiki
2019	インタビュー「もっとハッカーが必要だ」	atp magazin
2019	サイバー攻撃とダークネット - Jean Pereira インタビュー	Podcast "IT'S IN YOU"
2018	SEO-DAY：2018 年に Chrome をハックし SSL を回避する方法	Host Europe
2018	SEO-DAY 2018 のスーパーパネルでのセキュリティ講演	SEO-DAY / Online-Profession
2018	International Cyber Security Conference：Ethical Hacker と SECBIZ 創業者が登壇者として参加	DSS IT SEC / Riga