Jean Pereira

מחקר אבטחה · אבטחה התקפית · פיתוח Full-Stack

אני חוקר חולשות במערכות מורכבות ומפתח תוכנות אבטחה ומוצרים עצמאיים בתחומי אבטחת דפדפנים, מערכות משובצות ותעשייתיות, אוטומציה ובינה מלאכותית.

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

פרופיל

אני מוצא פרצות אבטחה במקום שבו אחרים מפסיקים לחפש, ובונה תוכנה מאובטחת שפותרת בעיות מורכבות.

עבודתי כוללת חולשות במוצרים ובטכנולוגיות של **Microsoft**, **Google**, **Apple**, **Siemens** ו-**Nokia**, וכן פרויקטים שונים בתחום הטכנולוגיה הרפואית. כיום אני מתמקד במחקר אבטחה ובהנדסת תוכנה.

אני גם היוצר של **Veloce**. אפשר ליצור איתי קשר דרך טופס יצירת הקשר או ישירות ב־LinkedIn.

עיקרי הדברים

ארבע חולשות יום אפס ב-Siemens: מערכות אזעקה וגלאי אש הועברו לשליטה מרחוק

השתלטתי מרחוק באופן מלא על מערכות אזעקה וגלאי אש של Siemens. הניצול שפיתחתי העניק לי גישת root, כלומר הרשאות המערכת הגבוהות ביותר, ללא פרטי כניסה, לחיצה או כל מעורבות אחרת של הקורבן.

פיתחתי שרשרת ניצול המשלבת ארבע חולשות שלא היו מוכרות והוכחתי בפועל השתלטות מלאה. מדובר בשליטה בטכנולוגיית התרעה קריטית לבטיחות.

Siemens אישרה את ארבעת הממצאים תחת CVE-2024-47904, CVE-2024-47903, CVE-2024-47902, CVE-2024-47901. הניצול קיבל ציון CVSS 10.0, רמת החומרה המרבית האפשרית.

חולשות יום אפס בבתי חולים: סוגי דם שונו, התרעות אק״ג ומערכות אוורור כובו

בבדיקת אבטחה גיליתי 22 חולשות לא מוכרות במכשירים של שנים עשר יצרנים והדגמתי תקיפות באמצעות ניצולים פעילים: כיבוי התרעות אק״ג, הפסקת אוורור בחדרי ניתוח סטריליים ושינוי סוגי דם ונתוני אלרגיות. פיתחתי גם מעקפי SOP/CORS והדגמתי תקיפות מרחוק על התקנים פנימיים שאינם נגישים ישירות מהאינטרנט.

היצרנים שנבדקו כוללים את ZEISS, MOXA, Zebra, Dedalus Labor ו-Tetronik. לפי כתבת Golem מ-2024, ההתקנים הושמשו באלפי בתי חולים ומוסדות רפואיים נוספים. תיאמתי דיווח ליצרנים וסייעתי בתיקון. עיתונאים ליוו את התהליך כולו, מהדיווח ליצרנים ועד לסיוע שלי בתיקון החולשות.

חולשות ביותר מ-40 רשויות, ב-OBI, ב-REWE ובמכון פראונהופר

חשפתי חולשות ב-45 רשויות מקומיות וחברות ודיווחתי לאחראים. ב-OBI חולשת רשת אפשרה חטיפת הפעלות משתמש וגישה למידע ממערכת ניהול התוכן הפנימית.

רשויות רבות תיקנו את החולשות. OBI הסירה את האתר בעקבות המחלוקת הציבורית. Golem ו-WirtschaftsWoche תיעדו את המחקר ואת תגובות החברות.

ניסיון

יוני 2023 - היום

CEO · CTO · CYTRES GmbH

ייסדתי וניהלתי את החברה תוך התמקדות בפיתוח תוכנה ובמחקר סייבר.

דצמ׳ 2016 - אוג׳ 2019

מדריך סייבר · Rotterdam · CIC (Cambridge Innovation Center), הולנד

העברתי סדנאות סייבר והדרכות טכניות.

דצמ׳ 2016 - אוג׳ 2019

יועץ אבטחה בכיר · Rotterdam · Base Cyber Security, הולנד

ניהלתי את הצוות הטכני והכשרתי עובדים חדשים עד לרמה הטכנית הנדרשת.

2019

מייסד · CEO · CTO · Secbiz IT Security GmbH

- מייסד ומוביל טכני של חברת סייבר.
- מחקר וייעוץ באבטחת מערכות תעשייתיות/OT ואפליקציות.
- הדגמת תקיפת SCADA חיה ביריד Hannover Messe בשנת 2019.

Veloce

Veloce הוא סביבת הריצה שלי ל-JavaScript/TypeScript עבור agentic coding: פלטפורמת יעד שעליה סוכני קוד יכולים לייצר יישומים מלאים, קריאים, ניתנים לביקורת ומוכנים להרצה מיידית, בלי להרכיב קודם תלותי npm, frameworks, כלי build ושכבות deployment.

סביבת הריצה כוללת את אבני הבניין החשובות: sandbox מגביל ומודל הרשאות, שרת HTTP, SQLite ו-PostgreSQL עם ORM ואחסון KV, יכולות דפדפן ו-desktop ואריזה לקובץ native עצמאי. נתיבים עתירי חישוב יכולים לעבור מ-JavaScript/TypeScript ל-native kernels מבוססי Rust או ל-WebAssembly. המטרה היא תוכנה שסוכנים יכולים לייצר באופן אמין, בני אדם עדיין יכולים להבין ומערכות יכולות להריץ עם כמה שפחות חלקים נעים.

מומחיות

מערכות משובצות, OT וציוד רפואי

מחקר חולשות בקושחה ובמכשירים מחוברים: מערכות גילוי אש, בקרים תעשייתיים (SCADA), ציוד בתי חולים ומכשור רפואי.

פיתוח exploits

מחולשת memory corruption בודדת ועד שרשרת exploit מלאה עם גישת root מרחוק.

אבטחת דפדפנים ו-web

עקיפות SOP/CORS, נתיבי תקיפה למכשירים ברשתות פנימיות, XSS ואבטחת יישומים.

חשיפה אחראית

דיווח ותיאום עם יצרנים ומפעילים, מחברות גדולות ועד רשויות עירוניות, כולל תמיכה בתיקון.

כלים עצמאיים

כלים ואוטומציה לאיתור חולשות ולבדיקות חדירה, כולל workflow בסיוע AI. יוצר Veloce JavaScript/TypeScript runtime.

מחקר

שנה	מחקר / חולשה	מקור
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	רישום CISA ב-CIRCL
2013	Apple Motion - CVE-2013-6114 - חולשת אבטחה	Apple
2014	Apple Web Server - מחקר אבטחה, פברואר 2014	Apple
2012	Nokia Hall of Fame - מחקר אבטחה, דצמבר 2012	Nokia
2012	Metasploit מודול - Android Browser DoS - CVE-2012-6301	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	ארכיון Bugtraq
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

תקשורת

שנה	כתבה מקורית	גוף תקשורת
2025	סיקור של גילוי אחראי ב-Securitas / Marvelit	Security-Insider

שנה	כתבה מקורית	גוף תקשורת
2022	קטע רדיו על אבטחת סייבר והאקינג אתי	WDR
2024	שיחת מומחים של ÖAG: אבטחה 4.0 - אבטחת סייבר והגנה באמצעות בינה מלאכותית	medianet (אוסטריה)
2024	פרצות אבטחה בבתי חולים: מטופלים בסיכון	Golem
2024	SOP/CORS בדפדפן והתקנים ברשת הפנימית	CYTRES Research
2024	הודעת אבטחה פומבית של Jean Pereira עם עדכון מתועד על התיקון	Volksbank / Sparda Bank (Responsible Disclosure)
2023	שיחת מומחים עם מזכיר המדינה טורסקי על דיגיטציה, בינה מלאכותית ואבטחת סייבר	KURIER (אוסטריה)
2023	השתתפות כמומחה אבטחת סייבר ב-ÖAG Super Tuesday	LEADERSNET (אוסטריה)
2022	פודקאסט #51: Ethical Hacker - מחקר אבטחה והמסלול המקצועי	IDG TechTalk / COMPUTERWOCHE
2022	פרצת אבטחת IT בעיריית קלן	Kölner Stadt-Anzeiger
2022	נציבת הגנת המידע חוקרת בעקבות התעלמות מפרצת אבטחה שדווחה	WirtschaftsWoche
2022	גילוי אחראי / 45 ארגונים	Golem
2022	דיווח על OBI ורשויות ציבוריות	connect professional
2020	הרצאה מרכזית על אבטחת דפדפנים ויישומים	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: האקינג SCADA/ICS בשידור חי	Hannover Messe / MittelstandsWiki
2019	ראיון: "אנחנו צריכים יותר האקרים"	atp magazin
2019	מתקפות סייבר ודארקנט - ראיון עם Jean Pereira	"Podcast "IT'S IN YOU
2018	SEO-DAY: כיצד לפרוץ ל-Chrome ולעקוף SSL בשנת 2018	Host Europe
2018	הרצאת אבטחה בסופר-פאנל של SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker ומייסד SECBIZ ברשימת המרצים	DSS IT SEC / Riga