Jean Pereira

أبحاث أمنية · أمن هجومي · تطوير Full-Stack

أبحث عن الثغرات في الأنظمة المعقدة وأطوّر برمجيات أمنية ومنتجات خاصة بي في مجالات أمن المتصفحات والأنظمة المضمنة والصناعية والأتمتة والذكاء الاصطناعي.

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

---

الملف

أجد الثغرات الأمنية حيث يتوقف الآخرون عن البحث، وأطوّر برمجيات آمنة تحل مشكلات معقّدة.

تشمل أعمالي ثغرات في منتجات وتقنيات **Siemens** و**Apple** و**Google** و**Microsoft** و**Nokia**، إضافة إلى مشاريع مختلفة في مجال التقنيات الطبية. ينصب تركيزي حاليًا على أبحاث الأمن وهندسة البرمجيات.

أنا أيضًا مطوّر **Veloce**. يمكنك التواصل معي عبر نموذج التواصل أو مباشرةً على LinkedIn.

أبرز النقاط

أربع ثغرات يوم صفر لدى **Siemens**: السيطرة عن بُعد على أنظمة الإنذار وكاشفات الحريق

سيطرت بالكامل عن بُعد على أنظمة الإنذار وكاشفات الحريق من Siemens. منحنى الاستغلال الذي طوّرته صلاحيات root، أي أعلى صلاحيات النظام، دون بيانات دخول أو نقرة أو أي تفاعل من الضحية.

طوّرت سلسلة استغلال تجمع أربع ثغرات لم تكن معروفة، وأثبتّ السيطرة الكاملة عمليًا. كان الأمر يتعلق بالتحكم في تقنية إنذار بالغة الأهمية للسلامة.

أكدت Siemens النتائج الأربع تحت المعرّفات CVE-2024-47904, CVE-2024-47903, CVE-2024-47902, CVE-2024-47901.

حصل الاستغلال على تقييم CVSS 10.0، أي أقصى درجة خطورة ممكنة.

ثغرات يوم صفر في المستشفيات: التلاعب بفصائل الدم وتعطيل إنذارات تخطيط القلب وأجهزة التهوية عمليًا

خلال تقييم أمني اكتشفت 22 ثغرة غير معروفة في أجهزة اثنى عشر مصنّعًا وأثبتّ الهجمات باستغلالات فعلية: تعطيل إنذارات تخطيط القلب، وقطع تهوية غرف العمليات المعقّمة، والتلاعب بفصائل الدم وبيانات الحساسية. كما طوّرت طرقًا لتجاوز SOP/CORS وأثبتّ هجمات عن بُعد على أجهزة داخلية غير متاحة مباشرة من الإنترنت.

شملت الشركات التي فحصت أنظمتها ZEISS وMOXA وZebra وDedalus Labor وTetronik. وبحسب تقرير Golem لعام 2024، كانت الأجهزة المعنية مستخدمة في آلاف المستشفيات والمنشآت الطبية الأخرى. نسّقت الإفصاح للمصنّعين ودعمت معالجة الثغرات. رافق الصحفيون العملية كاملة، من إبلاغ المصنّعين إلى دعمي لهم في معالجة الثغرات.

ثغرات لدى أكثر من **40** جهة حكومية و**OBI** و**REWE** ومعهد فراونهوفر

اكتشفت ثغرات لدى 45 إدارة بلدية وشركة وأبلغت المسؤولين عنها. لدى OBI، أتاحت ثغرة ويب الاستيلاء على جلسات المستخدمين وقراءة معلومات من نظام إدارة المحتوى الداخلي.

عالجت بلديات كثيرة الثغرات. وأوقفت OBI الموقع المعني بعد الجدل العلني. وثّقت Golem وWirtschaftsWoche البحث وتعامل الشركات مع النتائج.

الخبرة

يونيو 2023 - حتى الآن

CEO · CTO · CYTRES GmbH

أسست الشركة وقدتها مع التركيز على تطوير البرمجيات وأبحاث الأمن السيبراني.

ديسمبر 2016 - أغسطس 2019

مدرّس للأمن السيبراني · CIC (Cambridge Innovation Center) · Rotterdam, هولندا

قدّمت ورش عمل في الأمن السيبراني ودورات تدريبية تقنية.

ديسمبر 2016 - أغسطس 2019

مستشار أمني أول · Base Cyber Security · Rotterdam, هولندا

قدت الفريق التقني ودرّبت الموظفين الجدد حتى الوصول إلى المستوى التقني المطلوب.

2019

المؤسس · CEO · CTO · Secbiz IT Security GmbH

- مؤسس وقائد تقني لشركة متخصصة في الأمن السيبراني.
- أبحاث واستشارات في أمن الأنظمة الصناعية/OT والتطبيقات.
- عرض مباشر لاختراق نظام SCADA في معرض Hannover Messe عام 2019.

Veloce

Veloce هو بيئة تشغيل JavaScript/TypeScript التي طورتها للبرمجة الوكيلية: منصة هدف يستطيع عليها وكلاء البرمجة إنشاء تطبيقات كاملة قابلة للقراءة والمراجعة والتشغيل مباشرة، من دون الحاجة أولاً إلى تجميع حزم npm وأطر العمل وأدوات البناء وطبقات النشر.

تتضمن بيئة التشغيل المكونات الأساسية مباشرة: sandbox مقيد ونموذج صلاحيات، خادم HTTP، وSQLite وPostgreSQL مع ORM ومخزن KV، وقدرات للمتصفح وسطح المكتب، وإمكانية التغليف في ملف تنفيذي native مستقل. ويمكن نقل المسارات كثيفة الحساب من JavaScript/TypeScript إلى kernels أصلية مبنية على Rust أو إلى WebAssembly. الهدف هو برمجيات يمكن للوكلاء توليدها بصورة موثوقة، ويستطيع البشر فهمها، وتستطيع الأنظمة تشغيلها بأقل عدد ممكن من الأجزاء المتحركة.

المهارات

الأنظمة المضمنة وOT والتقنية الطبية

بحث الثغرات في البرامج الثابتة والأجهزة المتصلة: أنظمة إنذار الحريق، وحدات التحكم الصناعية (SCADA)، ومعدات المستشفيات والأجهزة الطبية.

تطوير الاستغلالات

من ثغرة memory corruption منفردة إلى سلسلة استغلال كاملة تمنح وصول root عن بُعد.

أمن المتصفحات والويب

تجاوزات SOP/CORS، ومسارات الهجوم إلى الأجهزة داخل الشبكات الداخلية، وXSS وأمن التطبيقات.

الإفصاح المسؤول

الإبلاغ والتنسيق مع الشركات المصنعة والمشغلين، من الشركات الكبرى إلى الإدارات البلدية، بما في ذلك دعم عملية الإصلاح.

أدواتي الخاصة

أدوات وأتمتة لاكتشاف الثغرات واختبارات الاختراق، بما في ذلك workflow مدعومة بالذكاء الاصطناعي. مؤلف /runtime JavaScript TypeScript Veloce.

الأبحاث

السنة	البحث / الثغرة	المصدر
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	إدخال CISA لدى CIRCL
2013	Apple Motion - CVE-2013-6114 - ثغرة أمنية	Apple
2014	Apple Web Server - أبحاث أمنية, فبراير 2014	Apple
2012	Nokia Hall of Fame - أبحاث أمنية, ديسمبر 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - وحدة Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	أرشيف 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

الصحافة

السنة	المنشور الأصلي	الوسيلة
2025	تغطية الإفصاح المسؤول لدى Securitas / Marvelit	Security-Insider
2022	مداخلة إذاعية حول الأمن السيبراني والاختراق الأخلاقي	WDR
2024	حوار خبراء ÖAG: الأمن 4.0 - الأمن السيبراني والدفاع بالذكاء الاصطناعي	medianet (النمسا)
2024	ثغرات أمنية في المستشفيات: المرضى في خطر	Golem
2024	SOP/CORS في المتصفح وأجهزة الشبكة الداخلية	CYTRES Research
2024	إشعار أمني علني من Jean Pereira مع تحديث موثّق حول المعالجة	Volksbank / Sparda Bank (Responsible Disclosure)
2023	حوار خبراء مع سكرتير الدولة تورسكي حول الرقمنة والذكاء الاصطناعي والأمن السيبراني	KURIER (النمسا)
2023	المشاركة بصفته خبيرًا في الأمن السيبراني في ÖAG Super Tuesday	LEADERSNET (النمسا)
2022	بودكاست #51: Ethical Hacker - أبحاث الأمن والمسار المهني	IDG TechTalk / COMPUTERWOCHE
2022	ثغرة أمنية في تقنية المعلومات لدى مدينة كولونيا	Kölner Stadt-Anzeiger
2022	مفوّضة حماية البيانات تحقق بعد تجاهل ثغرة أمنية تم الإبلاغ عنها	WirtschaftsWoche
2022	الإفصاح المسؤول / 45 جهة	Golem
2022	تقرير عن OBI والجهات الحكومية	connect professional
2020	كلمة رئيسية حول أمن المتصفحات والتطبيقات	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: اختراق SCADA/ICS مباشر	Hannover Messe / MittelstandsWiki
2019	مقابلة «نحتاج إلى مزيد من المخترقين»	atp magazin
2019	هجمات سيبرانية ودارك نت - مقابلة مع Jean Pereira	"Podcast "IT'S IN YOU
2018	SEO-DAY: كيفية اختراق Chrome وتجاوز SSL في 2018	Host Europe
2018	محاضرة أمنية ضمن الجلسة الكبرى في SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker ومؤسس SECBIZ ضمن قائمة المتحدثين	DSS IT SEC / Riga