Jean Pereira

Güvenlik araştırması · Saldırı güvenliği · Full-stack geliştirme

Karmaşık sistemlerdeki güvenlik açıklarını araştırıyor; tarayıcı güvenliği, gömülü ve endüstriyel sistemler, otomasyon ve yapay zekâ alanlarında güvenlik yazılımı ve kendi ürünlerimi geliştiriyorum.

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

Profil

Başkalarının aramayı bıraktığı yerde güvenlik açıkları buluyor ve karmaşık sorunları çözen güvenli yazılımlar geliştiriyorum.

Çalışmalarım **Siemens**, **Apple**, **Google**, **Microsoft** ve **Nokia** ürün ve teknolojilerindeki güvenlik açıklarının yanı sıra tıbbi teknoloji alanındaki çeşitli projeleri da kapsıyor. Şu anda güvenlik araştırmalarına ve yazılım mühendisliğine odaklanıyorum.

Ayrıca **Veloce** projesinin yazarıyım. Bana iletişim formu üzerinden veya doğrudan LinkedIn üzerinden ulaşabilirsin.

Öne çıkanlar

Siemens'te dört sıfır gün açığı: alarm sistemleri ve yangın dedektörleri uzaktan ele geçirildi

Siemens alarm sistemlerinin ve yangın dedektörlerinin kontrolünü uzaktan tamamen ele geçirdim. Exploitim bana root erişimi, yani en yüksek sistem yetkilerini verdi. Giriş bilgisi, tıklama veya mağdurun başka bir etkileşimi gerekmiyordu.

Daha önce bilinmeyen dört açığı birleştiren bir exploit zinciri geliştirdim ve tam kontrolü uygulamalı olarak gösterdim. Söz konusu olan, güvenlik açısından kritik alarm teknolojisinin kontrolüydü.

Siemens dört bulguyu CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904 olarak doğruladı. Exploitin aldığı puan CVSS 10.0, mümkün olan en yüksek kritiklik düzeyidir.

Hastanelerde sıfır gün açıkları: kan grupları değiştirildi, EKG alarmları ve havalandırma cihazları kapatıldı

Bir güvenlik incelemesinde on iki üreticinin cihazlarında daha önce bilinmeyen 22 açık keşfettim ve saldırıları çalışan exploitlerle gösterdim: EKG alarmlarını kapatma, steril ameliyathane havalandırmasını kesme, kan grubu ve alerji kayıtlarını değiştirme. Geliştirdiğim SOP/CORS atlatmalarıyla internete doğrudan açık olmayan iç ağ cihazlarına uzaktan saldırıları da gösterdim.

İncelenen üreticiler arasında ZEISS, MOXA, Zebra, Dedalus Labor ve Tetronik bulunuyor. Golem'in 2024 tarihli haberine göre etkilenen cihazlar binlerce başka hastane ve tıbbi tesiste kullanılıyordu. Üreticilere bildirimleri koordine ettim ve düzeltmeleri destekledim. Gazeteciler, üreticilere bildirimden düzeltmelere verdiğim desteğe kadar tüm süreci izledi.

40'tan fazla kamu kurumunda, OBI, REWE ve Fraunhofer Enstitüsü'nde güvenlik açıkları

45 belediye ve şirkette açıklar keşfettim ve sorumlulara bildirdim. OBI'de bir web açığı, kullanıcı oturumlarını ele geçirmeye ve dahili içerik yönetim sisteminden bilgi okumaya olanak veriyordu.

Birçok belediye açıkları kapattı. OBI, kamuoyundaki tartışmanın ardından ilgili siteyi kapattı. Golem ve WirtschaftsWoche araştırmayı ve şirketlerin tepkilerini belgeledi.

Deneyim

Haz 2023 - günümüz

CEO · CTO · CYTRES GmbH
Şirketi kurup yönettim; odak noktası yazılım geliştirme ve siber güvenlik araştırmasıydı.

Ara 2016 - Ağu 2019

Siber güvenlik eğitmeni · CIC (Cambridge Innovation Center) · Rotterdam, Hollanda
Siber güvenlik atölyeleri ve teknik eğitimler düzenledim.

Ara 2016 - Ağu 2019

Kıdemli güvenlik danışmanı · Base Cyber Security · Rotterdam, Hollanda
Teknik ekibi yönettim ve yeni çalışanları gerekli teknik seviyeye ulaşana kadar eğittim.

2019

Kurucu · CEO · CTO · Secbiz IT Security GmbH
- Bir siber güvenlik şirketinin kurucusu ve teknik lideri.
- Endüstriyel/OT ve uygulama güvenliği araştırması ve danışmanlık.
- Hannover Messe 2019'da canlı SCADA saldırısı gösterimi.

Veloce

Veloce, agentic coding için geliştirdiğim JavaScript/TypeScript runtime'ıdır: kodlama ajanlarının npm bağımlılıklarını, frameworkleri, build araçlarını ve deployment glue'yu önce bir araya getirmeden okunabilir, denetlenebilir ve doğrudan çalıştırılabilir tam uygulamalar üretebildiği bir hedef platformdur.

Runtime gerekli yapı taşlarını doğrudan sunar: kısıtlayıcı sandbox ve izin modeli, HTTP sunucusu, ORM ve KV deposuyla SQLite ve PostgreSQL, tarayıcı ve masaüstü yetenekleri ve bağımsız native binary olarak paketleme. Hesaplama yoğun yollar JavaScript/TypeScript'ten Rust tabanlı native kernel'lara veya WebAssembly'ye aktarılabilir. Amaç; ajanların güvenilir biçimde üretebildiği, insanların hâlâ anlayabildiği ve sistemlerin mümkün olduğunca az hareketli parçayla çalıştırabildiği yazılımdır.

Uzmanlık

Gömülü sistemler, OT ve medikal teknoloji

Firmware ve bağlı cihazlarda güvenlik açığı araştırması: yangın alarm sistemleri, endüstriyel kontrol sistemleri (SCADA), hastane ve tıbbi cihazlar.

Exploit geliştirme

Tek bir memory corruption hatasından uzaktan root erişimi sağlayan tam bir exploit zincirine kadar.

Tarayıcı ve web güvenliği

SOP/CORS bypassları, iç ağdaki cihazlara giden saldırı yolları, XSS ve uygulama güvenliği.

Sorumlu açıklama

Üreticiler ve işletmecilerle, büyük şirketlerden belediye idarelerine kadar bildirim ve koordinasyon, düzeltme desteği dahil.

Kendi araçlarım

Güvenlik açığı keşfi ve penetration testing için araçlar ve otomasyon, AI destekli workflow'lar dahil. Veloce JavaScript/TypeScript runtime'ının yazarı.

Araştırma

Yıl	Araştırma / zafiyet	Kaynak
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 üzerindeki CISA kaydı
2013	Apple Motion - CVE-2013-6114 - güvenlik açığı	Apple
2014	Apple Web Server - güvenlik araştırması, Şubat 2014	Apple
2012	Nokia Hall of Fame - güvenlik araştırması, Aralık 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit modülü	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq arşivi
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

Yıl	Araştırma / zafiyet	Kaynak
2012	plow .plowrc - Buffer Overflow - BID 54290	Bugtraq
2012	Internet Explorer - XSS Filter Bypass - Exploit-DB 22100	VulDB

Basın

Yıl	Özgün makale	Yayın
2025	Securitas / Marvelit responsible disclosure sürecine ilişkin haber	Security-Insider
2022	Siber güvenlik ve etik hackerlık üzerine radyo yayını	WDR
2024	ÖAG uzman söyleşisi: Güvenlik 4.0 - siber güvenlik ve yapay zekâ destekli savunma	medianet (Avusturya)
2024	Hastanelerde güvenlik açıkları: hastalar risk altında	Golem
2024	Tarayıcı SOP/CORS ve iç ağ cihazları	CYTRES Research
2024	Jean Pereira'nın belgelenmiş düzeltme güncellemesi içeren kamuya açık güvenlik bildirimi	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Devlet Sekreteri Tursky ile dijitalleşme, yapay zekâ ve siber güvenlik üzerine uzman söyleşisi	KURIER (Avusturya)
2023	ÖAG Super Tuesday etkinliğine siber güvenlik uzmanı olarak katılım	LEADERSNET (Avusturya)
2022	Podcast #51: Ethical Hacker - güvenlik araştırmaları ve kariyer yolu	IDG TechTalk / COMPUTERWOCHE
2022	Köln Belediyesi'nde BT güvenlik açığı	Kölner Stadt-Anzeiger
2022	Veri koruma komiseri, bildirilen bir güvenlik açığının görmezden gelinmesini soruşturuyor	WirtschaftsWoche
2022	Responsible disclosure / 45 kuruluş	Golem
2022	OBI ve kamu kurumları hakkında haber	connect professional
2020	Tarayıcı ve uygulama güvenliği üzerine keynote	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: canlı SCADA/ICS hacking	Hannover Messe / MittelstandsWiki
2019	Röportaj: "Daha fazla hackera ihtiyacımız var"	atp magazin
2019	Siber saldırılar & darknet - Jean Pereira ile röportaj	Podcast "IT'S IN YOU"
2018	SEO-DAY: 2018'de Chrome nasıl hacklenir ve SSL nasıl aşılır	Host Europe
2018	SEO-DAY 2018 superpanelinde güvenlik sunumu	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker ve SECBIZ kurucusu konuşmacılar arasında	DSS IT SEC / Riga