Jean Pereira

Investigación de seguridad · Seguridad ofensiva · Ingeniería full-stack

Investigo vulnerabilidades en sistemas complejos y desarrollo software de seguridad y productos propios en seguridad de navegadores, sistemas embebidos e industriales, automatización e inteligencia artificial.

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

Perfil

Encuentro vulnerabilidades de seguridad donde otros dejan de buscar y desarrollo software seguro que resuelve problemas complejos.

Entre mis trabajos se incluyen vulnerabilidades en productos y tecnologías de **Siemens**, **Apple**, **Google**, **Microsoft** y **Nokia**, así como diversos proyectos en el ámbito de la tecnología médica. Actualmente me centro en la investigación de seguridad y la ingeniería de software.

También soy autor de **Veloce**. Puedes contactar conmigo a través del formulario de contacto o directamente en LinkedIn.

Destacados

Cuatro zero-days en Siemens: sistemas de alarma y detectores de incendios controlados a distancia

Tomé el control completo a distancia de sistemas de alarma y detectores de incendios de Siemens. Mi exploit me concedió acceso root, los máximos privilegios del sistema, sin credenciales, clics ni otra intervención de la víctima.

Desarrollé una cadena de explotación combinando cuatro vulnerabilidades desconocidas y demostré el control completo en la práctica. Se trataba del control de tecnología de alarmas esencial para la seguridad.

Siemens confirmó los cuatro hallazgos, CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. El exploit recibió CVSS 10.0, la máxima criticidad posible.

Zero-days en hospitales: grupos sanguíneos manipulados, alarmas ECG y equipos de ventilación desactivados

En una evaluación descubrí 22 vulnerabilidades desconocidas en dispositivos de doce fabricantes y demostré los ataques con exploits funcionales: desactivar alarmas ECG, interrumpir la ventilación de quirófanos estériles y manipular grupos sanguíneos y registros de alergias. También desarrollé bypasses SOP/CORS para demostrar ataques remotos contra dispositivos internos sin acceso directo desde Internet.

Entre los fabricantes investigados figuran ZEISS, MOXA, Zebra, Dedalus Labor y Tetronik. Según el reportaje de Golem de 2024, los dispositivos afectados se utilizaban en miles de otros hospitales y centros médicos. Coordiné la divulgación y apoyé la corrección. Periodistas acompañaron todo el proceso, desde la notificación a los fabricantes hasta mi apoyo a la corrección.

Vulnerabilidades en más de 40 administraciones, OBI, REWE y el Instituto Fraunhofer

Descubrí vulnerabilidades en 45 administraciones municipales y empresas y las comuniqué a sus responsables. En OBI, una vulnerabilidad web permitía secuestrar sesiones y acceder a información del sistema interno de gestión de contenidos.

Muchas administraciones corrigieron los fallos. OBI retiró el sitio afectado tras la controversia pública. Golem y WirtschaftsWoche documentaron la investigación y las respuestas de las empresas.

Experiencia

jun 2023 - actualidad

CEO · CTO · CYTRES GmbH
Fundé y dirigí la empresa con un enfoque en desarrollo de software e investigación en ciberseguridad.

dic 2016 - ago 2019

Tutor de ciberseguridad · CIC (Cambridge Innovation Center) · Rotterdam, Países Bajos
Impartí talleres de ciberseguridad y formación técnica.

dic 2016 - ago 2019

Asesor sénior de seguridad · Base Cyber Security · Rotterdam, Países Bajos
Dirigí el equipo técnico y formé a nuevos empleados hasta alcanzar el nivel técnico requerido.

2019

Fundador · CEO · CTO · Secbiz IT Security GmbH

- Fundación y dirección técnica de una empresa de seguridad; investigación de seguridad, consultoría y pruebas de penetración.
- Enfoque en seguridad industrial/OT, seguridad web y de aplicaciones, y análisis de vulnerabilidades.
- Ponencia y demostración en directo en Hannover Messe 2019 sobre ataques contra sistemas de control SCADA industriales.

Veloce

Veloce es mi runtime de JavaScript/TypeScript para programación agéntica: una plataforma objetivo en la que los agentes de código pueden crear aplicaciones completas, legibles, auditables y ejecutables directamente, sin tener que montar primero dependencias npm, frameworks, herramientas de build y capas de despliegue.

El runtime incluye directamente las piezas importantes: un sandbox y un modelo de permisos restrictivos, servidor HTTP, SQLite y PostgreSQL con ORM y almacenamiento KV, funciones de navegador y escritorio, y empaquetado en un binario nativo autónomo. Las rutas de cálculo intensivo pueden trasladarse desde JavaScript/TypeScript a kernels nativos respaldados por Rust o a WebAssembly. El objetivo es software que los agentes puedan generar de forma fiable, que las personas sigan pudiendo entender y que los sistemas ejecuten con el menor número posible de piezas móviles.

Competencias

Sistemas embebidos, OT y tecnología médica

Investigación de vulnerabilidades en firmware y dispositivos conectados: sistemas de detección de incendios, controladores industriales (SCADA) y equipos hospitalarios y médicos.

Desarrollo de exploits

Desde un fallo individual de corrupción de memoria hasta una cadena completa de explotación con acceso root remoto.

Seguridad de navegadores y web

Evasiones de SOP/CORS, rutas de ataque contra dispositivos de redes internas, XSS y seguridad de aplicaciones.

Divulgación responsable

Notificación y coordinación con fabricantes y operadores, desde grandes empresas hasta administraciones municipales, incluida la asistencia durante la corrección.

Herramientas propias

Herramientas y automatización para el descubrimiento de vulnerabilidades y las pruebas de penetración, incluidos flujos de trabajo asistidos por IA. Autor de la runtime JavaScript/TypeScript Veloce.

Investigación

Año	Investigación / vulnerabilidad	Fuente
2024	Siemens ProductCERT, SSA-333468 - CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904; ejecución remota de código como root	Siemens
2024	Siemens InterMesh - aviso ICS de CISA ICSA-24-303-01	Entrada de CISA en CIRCL
2013	Apple Motion - CVE-2013-6114 - vulnerabilidad en Apple Motion	Apple
2014	Apple Web Server - investigación de seguridad, febrero de 2014	Apple
2012	Nokia Hall of Fame - investigación de seguridad, diciembre de 2012	Nokia
2012	Denegación de servicio en Android Browser - CVE-2012-6301 - módulo de Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - corrupción de memoria / denegación de servicio	Archivo de Bugtraq
2012	PhpTax - CVE-2012-10037 - inyección remota de comandos	OpenCVE

Año	Investigación / vulnerabilidad	Fuente
2012	b2ePMS - CVE-2012-6626 - inyección SQL / elusión de autenticación	Bugtraq
2012	HCView - ejecución remota de código - BID 55819	Bugtraq
2012	DomsHttpd - denegación de servicio remota - BID 54478	Bugtraq
2012	CommPort - inyección SQL - BID 55239	Bugtraq
2012	Arctic Torrent - corrupción de memoria - BID 55833	Bugtraq
2012	plow .plowrc - desbordamiento de búfer - BID 54290	Bugtraq
2012	Internet Explorer - elusión del filtro XSS - Exploit-DB 22100	VulDB

Prensa

Año	Publicación original	Medio
2025	Cobertura sobre la divulgación responsable en Securitas / Marvelit	Security-Insider
2022	Reportaje radiofónico sobre ciberseguridad y hacking ético	WDR
2024	Charla de expertos de la ÖAG: Seguridad 4.0 - ciberseguridad y defensa mediante IA	medianet (Austria)
2024	Vulnerabilidades de seguridad en hospitales: pacientes en riesgo	Golem
2024	SOP/CORS del navegador y dispositivos de la red interna	CYTRES Research
2024	Aviso público de seguridad de Jean Pereira con actualización documentada sobre la corrección	Volksbank / Sparda Bank (divulgación responsable)
2023	Charla de expertos con el secretario de Estado Tursky sobre digitalización, IA y ciberseguridad	KURIER (Austria)
2023	Participación como experto en ciberseguridad en el ÖAG Super Tuesday	LEADERSNET (Austria)
2022	Podcast #51: Ethical Hacker - investigación de seguridad y trayectoria profesional	IDG TechTalk / COMPUTERWOCHE
2022	Vulnerabilidad de seguridad informática en la ciudad de Colonia	Kölner Stadt-Anzeiger
2022	La comisionada de protección de datos investiga tras ignorarse una vulnerabilidad de seguridad notificada	WirtschaftsWoche
2022	Divulgación responsable / 45 organizaciones	Golem
2022	Informe sobre OBI y administraciones públicas	connect professional
2020	Ponencia principal sobre seguridad de navegadores y aplicaciones	OMT - Conferencia de Marketing Online
2019	Foro de Seguridad Industrial: hacking de SCADA/ICS en directo	Hannover Messe / MittelstandsWiki
2019	Entrevista «Necesitamos más hackers»	atp magazin
2019	Ciberataques y darknet - entrevista con Jean Pereira	Podcast "IT'S IN YOU"
2018	SEO-DAY: cómo hackear Chrome y eludir SSL en 2018	Host Europe
2018	Ponencia de seguridad en el superpanel del SEO-DAY 2018	SEO-DAY / Online-Profession
2018	Conferencia Internacional de Ciberseguridad: Ethical Hacker y fundador de SECBIZ en el cartel de ponentes	DSS IT SEC / Riga