Jean Pereira

Tietoturvatutkimus · Hyökkäävä tietoturva · Full-stack-kehitys

Tutkin monimutkaisten järjestelmien haavoittuvuuksia ja kehitän tietoturvaohjelmistoja sekä omia tuotteita selain-, sulautettujen ja teollisten järjestelmien turvallisuuteen, automaatioon ja tekoälyyn.

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

Profiili

Löydän tietoturva-aukkoja sieltä, missä muut lopettavat etsimisen, ja rakennan turvallisia ohjelmistoja, jotka ratkaisevat monimutkaisia ongelmia.

Työni sisältää haavoittuvuuksia **Siemensin**, **Applen**, **Googlen**, **Microsoftin** ja **Nokian** tuotteissa ja teknologioissa sekä erilaisia lääketieteellisen tekniikan projekteja. Keskityn tällä hetkellä tietoturvatutkimukseen ja ohjelmistotekniikkaan.

Olen myös **Veloce**-ohjelmiston tekijä. Voit ottaa minuun yhteyttä yhteydenottolomakkeella tai suoraan LinkedIn-palvelussa.

Kohokohdat

Neljä nollapäivähaavoittuvuutta Siemensillä: hälytysjärjestelmät ja paloilmaisimet otettu haltuun etänä

Otin etänä täyden hallinnan Siemensin hälytysjärjestelmiin ja paloilmaisimiin. Exploitini antoi root-pääsyn eli korkeimmat järjestelmäoikeudet ilman kirjautumistietoja, napsautuksia tai uhrin muita toimia.

Kehitin neljä tuntematonta haavoittuvuutta yhdistävän exploit-ketjun ja osoitin täydellisen haltuunoton käytännössä. Kyse oli turvallisuuskriittisen hälytystekniikan hallinnasta.

Siemens vahvisti neljä löydöstä tunnisteilla CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Exploit sai luokituksen CVSS 10.0, suurin mahdollinen vakavuus.

Sairaaloiden nollapäivähaavoittuvuudet: veriryhmät muutettu, EKG-hälytykset ja ilmanvaihtolaitteet sammutettu

Tietoturvatutkimuksessa löysin 22 aiemmin tuntematonta haavoittuvuutta kahdentoista valmistajan laitteista ja osoitin hyökkäykset toimivilla exploiteilla: EKG-hälytysten sammuttaminen, steriilien leikkaussalien ilmanvaihdon keskeyttäminen sekä veriryhmä- ja allergiatietojen muuttaminen. Kehitin myös SOP/CORS-ohituksia ja osoitin etähyökkäykset sisäisiin laitteisiin, joihin ei ollut suoraa internetyhteyttä.

Tutkittuja valmistajia ovat ZEISS, MOXA, Zebra, Dedalus Labor ja Tetronik. Golemin vuoden 2024 reportaasin mukaan laitteita käytettiin tuhansissa muissa sairaaloissa ja hoitolaitoksissa. Koordinoin ilmoitukset ja tuin korjaamista. Toimittajat seurasivat koko prosessia valmistajille ilmoittamisesta korjaustyön tukemiseen.

Haavoittuvuuksia yli 40 viranomaisella, OBIssa, REWEssä ja Fraunhofer-instituutissa

Löysin haavoittuvuuksia 45 kunnasta ja yrityksestä ja ilmoitin niistä vastuuhenkilöille. OBIssa verkkosovelluksen haavoittuvuus mahdollisti käyttäjäistuntojen kaappaamisen ja sisäisen sisällönhallintajärjestelmän tietojen lukemisen.

Monet kunnat korjasivat virheet. OBI sulki kyseisen sivuston julkisen kiistan jälkeen. Golem ja WirtschaftsWoche dokumentoivat tutkimuksen ja yritysten reaktiot.

Kokemus

kesä 2023 - nykyhetki

CEO · CTO · CYTRES GmbH
Perustin ja johdin yritystä painottaen ohjelmistokehitystä ja kyberturvallisuustutkimusta.

joulu 2016 - elo 2019

Kyberturvallisuuden tutor · CIC (Cambridge Innovation Center) · Rotterdam, Alankomaat
Järjestin kyberturvallisuustyöpajoja ja teknisiä koulutuksia.

joulu 2016 - elo 2019

Vanhempi tietoturva-asiantuntija · Base Cyber Security · Rotterdam, Alankomaat
Johdin teknistä tiimiä sekä perehdytin ja koulutin uusia työntekijöitä vaaditulle tekniselle tasolle.

2019

Perustaja · CEO · CTO · Secbiz IT Security GmbH
- Kyberturvayrityksen perustaja ja tekninen johtaja.
- Tutkimus ja konsultointi teollisen/OT- ja sovellusturvan parissa.
- SCADA-hyökkäyksen live-esitys Hannover Messe -messuilla 2019.

Veloce

Veloce on JavaScript/TypeScript-ajoympäristöni agentic codingia varten: kohdealusta, jolla koodausagentit voivat tuottaa kokonaisia sovelluksia, jotka ovat luettavia, auditoitavia ja suoraan ajettavia ilman npm-riippuvuuksien, frameworkien, build-työkalujen ja deployment-liimauksen kokoamista.

Runtime sisältää olennaiset rakennuspalikat valmiina: rajoittavan sandbox- ja käyttöoikeusmallin, HTTP-palvelimen, SQLite- ja PostgreSQL-tuen ORM- ja KV-tallennuksella, selain- ja desktop-toiminnot sekä paketoinnin itsenäiseksi natiiviksi binääriksi. Laskennallisesti raskaat osat voidaan siirtää JavaScript/TypeScriptistä Rust-pohjaisiin natiivikernelihin tai WebAssemblyyn. Tavoitteena on ohjelmisto, jonka agentit voivat tuottaa luotettavasti, ihmiset edelleen ymmärtävät ja järjestelmät ajavat mahdollisimman vähillä liikkuvilla osilla.

Osaaminen

Sulautetut järjestelmät, OT ja lääketekniikka

Haavoittuvuustutkimus firmware- ja verkkolaitteissa: paloilmoitinjärjestelmät, teollisuuden ohjausjärjestelmät (SCADA), sairaala- ja lääkintälaitteet.

Exploit-kehitys

Yksittäisestä memory corruption -virheestä täydelliseen exploit-ketjuun, joka mahdollistaa etä-root-oikeudet.

Selain- ja verkkoturvallisuus

SOP/CORS-ohitukset, hyökkäyspolut sisäverkon laitteisiin, XSS ja sovellusturvallisuus.

Vastuullinen ilmoittaminen

Ilmoittaminen ja koordinointi valmistajien ja operaattorien kanssa suuryrityksistä kuntahallintoihin, mukaan lukien korjausten tukeminen.

Omat työkalut

Työkalut ja automaatio haavoittuvuuksien löytämiseen ja penetraatiotestaukseen, myös tekoälyavusteisina työnkulkuina. JavaScript/TypeScript-runtime Velocen tekijä.

Tutkimus

Vuosi	Tutkimus / haavoittuvuus	Lähde
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	CISA-merkintä CIRCLissä
2013	Apple Motion - CVE-2013-6114 - haavoittuvuus	Apple
2014	Apple Web Server - tietoturvatutkimus, helmikuu 2014	Apple
2012	Nokia Hall of Fame - tietoturvatutkimus, joulukuu 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - Metasploit-moduuli	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	Bugtraq-arkisto
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

Vuosi	Tutkimus / haavoittuvuus	Lähde
2012	plow .plowrc - Buffer Overflow - BID 54290	Bugtraq
2012	Internet Explorer - XSS Filter Bypass - Exploit-DB 22100	VulDB

Media

Vuosi	Alkuperäinen julkaisu	Media
2025	Raportointi responsible disclosure -prosessista Securitasilla / Marvelitilla	Security-Insider
2022	Radio-ohjelma kyberturvallisuudesta ja eettisestä hakkeroinnista	WDR
2024	ÖAG:n asiantuntijakeskustelu: Turvallisuus 4.0 - kyberturvallisuus ja tekoälypuolustus	medianet (Itävalta)
2024	Tietoturvahaavoittuvuuksia sairaaloissa: potilaat vaarassa	Golem
2024	Selaimen SOP/CORS ja sisäverkon laitteet	CYTRES Research
2024	Jean Pereiran julkinen tietoturvailmoitus ja dokumentoitu korjauspäivitys	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Asiantuntijakeskustelu valtiosihteeri Turskyn kanssa digitalisaatiosta, tekoälystä ja kyberturvallisuudesta	KURIER (Itävalta)
2023	Osallistuminen kyberturvallisuusasiantuntijana ÖAG Super Tuesday -tapahtumaan	LEADERSNET (Itävalta)
2022	Podcast #51: Ethical Hacker - tietoturvatutkimus ja urapolku	IDG TechTalk / COMPUTERWOCHE
2022	Kölnin kaupungin IT-tietoturvahaavoittuvuus	Kölner Stadt-Anzeiger
2022	Tietosuojavaltuutettu tutkii sivuutettua ilmoitusta tietoturva-aukosta	WirtschaftsWoche
2022	Responsible disclosure / 45 organisaatiota	Golem
2022	Raportti OBIsta ja viranomaisista	connect professional
2020	Keynote selainten ja sovellusten tietoturvasta	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: SCADA/ICS-hakkerointi livenä	Hannover Messe / MittelstandsWiki
2019	Haastattelu "Tarvitsemme lisää hakkereita"	atp magazin
2019	Kyberhyökkäykset & darknet - Jean Pereira haastattelussa	Podcast "IT'S IN YOU"
2018	SEO-DAY: miten Chrome hakkeroidaan ja SSL kierretään vuonna 2018	Host Europe
2018	Tietoturvaesitys SEO-DAY 2018:n superpaneelissa	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker ja SECBIZin perustaja puhujakaartissa	DSS IT SEC / Riga