Jean Pereira

Utafiti wa usalama · Offensive security · Uhandisi wa full-stack

Ninatafiti udhaifu katika mifumo changamano na kutengeneza programu za usalama pamoja na bidhaa zangu mwenyewe katika usalama wa vivinjari, mifumo iliyopachikwa na ya viwandani, otomatiki na AI.

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

Wasifu

Ninapata udhaifu wa usalama pale wengine wanapoacha kutafuta, na ninatengeneza programu salama zinazotatua matatizo changamano.

Kazi yangu inajumuisha udhaifu katika bidhaa na teknolojia za **Siemens**, **Apple**, **Google**, **Microsoft** na **Nokia**, pamoja na miradi mbalimbali katika teknolojia ya matibabu. Kwa sasa ninajikita katika utafiti wa usalama na uhandisi wa programu.

Mimi pia ni mtengenezaji wa **Veloce**. Unaweza kuwasiliana nami kupitia fomu ya mawasiliano au moja kwa moja kwenye LinkedIn.

Mambo muhimu

Zero-day nne katika Siemens: mifumo ya kengele na vigunduzi vya moto vimetwaliwa kwa mbali

Nilichukua udhibiti kamili kwa mbali wa mifumo ya kengele na vigunduzi vya moto vya Siemens. Exploit yangu ilinipa ufikiaji wa root, ruhusa za juu zaidi za mfumo, bila taarifa za kuingia, kubofya au ushiriki mwingine wa mwathiriwa.

Nilitengeneza mnyororo wa exploit unaounganisha udhaifu nne usiojulikana na kuonyesha udhibiti kamili kwa vitendo. Huu ulikuwa udhibiti wa teknolojia ya kengele muhimu sana kwa usalama.

Siemens ilithibitisha matokeo manne kama CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Exploit ilipata tathmini ya CVSS 10.0, kiwango cha juu kabisa cha ukali kinachowezekana.

Zero-day hospitalini: makundi ya damu yamebadilishwa, kengele za ECG na vifaa vya uingizaji hewa zimezimwa

Katika tathmini ya usalama niligundua udhaifu 22 usiojulikana katika vifaa ya wazalishaji kumi na wawili na kuonyesha mashambulizi kwa exploit zinazofanya kazi: kuzima kengele za ECG, kusimamisha uingizaji hewa wa vyumba tasa vya upasuaji na kubadilisha makundi ya damu na taarifa za mzio. Nilitengeneza pia njia za kupita SOP/CORS kuonyesha mashambulizi ya mbali dhidi ya vifaa vya ndani visivyofikika moja kwa moja kutoka intaneti.

Wazalishaji waliochunguzwa ni pamoja na ZEISS, MOXA, Zebra, Dedalus Labor na Tetronik. Kulingana na ripoti ya Golem ya 2024, vifaa vilitumika katika maelfu ya hospitali na vituo vingine vya matibabu. Niliratibu ufichuzi kwa wazalishaji na kusaidia marekebisho. Waandishi wa habari walifuatilia mchakato mzima, kuanzia taarifa kwa wazalishaji hadi msaada wangu katika marekebisho.

Udhaifu katika zaidi ya mamlaka 40 za umma, OBI, REWE na Taasisi ya Fraunhofer

Niligundua udhaifu katika manispaa na kampuni 45 na kuwaripoti wahusika. Kwa OBI, udhaifu wa wavuti uliwezesha kuteka vikao vya watumiaji na kusoma taarifa kutoka mfumo wa ndani wa usimamizi wa maudhui.

Manispaa nyingi zilirekebisha matatizo. OBI iliondoa tovuti husika baada ya mjadala wa umma. Golem na WirtschaftsWoche ziliandika kuhusu utafiti na majibu ya kampuni.

Uzoefu

Jun 2023 - sasa

CEO · CTO · CYTRES GmbH
Nilianzisha na kuongoza kampuni kwa kuzingatia maendeleo ya programu na utafiti wa usalama wa mtandao.

Des 2016 - Ago 2019

Mkufunzi wa usalama wa mtandao · CIC (Cambridge Innovation Center) · Rotterdam, Uholanzi
Niliendesha warsha za usalama wa mtandao na mafunzo ya kiufundi.

Des 2016 - Ago 2019

Mshauri mwandamizi wa usalama · Base Cyber Security · Rotterdam, Uholanzi
Niliongoza timu ya kiufundi na kuwafunza wafanyakazi wapya hadi kufikia kiwango cha kiufundi kinachohitajika.

2019

Mwanzilishi · CEO · CTO · Secbiz IT Security GmbH

- Mwanzilishi na kiongozi wa kiufundi wa kampuni ya usalama wa mtandao.
- Utafiti na ushauri kuhusu usalama wa viwandani/OT na programu.
- Onyesho la moja kwa moja la shambulio la SCADA kwenye Hannover Messe 2019.

Veloce

Veloce ni runtime yangu ya JavaScript/TypeScript kwa agentic coding: jukwaa lengwa ambalo mawakala wa coding wanaweza kutengeneza programu kamili zinazosomeka, kukaguliwa na kuendeshwa moja kwa moja bila kwanza kuunganisha npm dependencies, frameworks, build tooling na deployment glue.

Runtime ina vipengele muhimu vilivyojengewa ndani: sandbox na mfumo wa permissions wenye vizuizi, HTTP server, SQLite na PostgreSQL zenye ORM na KV store, uwezo wa browser na desktop, pamoja na packaging kuwa native binary inayojitegemea. Njia zenye mzigo mkubwa wa hesabu zinaweza kuhamishwa kutoka JavaScript/TypeScript kwenda native kernels zinazotegemea Rust au WebAssembly. Lengo ni software ambayo agents wanaweza kuzalisha kwa kutegemewa, binadamu bado wakaielewa, na mifumo ikaendesha kwa sehemu chache zinazobadilika kadiri iwezekanavyo.

Utaalamu

Embedded, OT na vifaa vya matibabu

Utafiti wa udhaifu katika firmware na vifaa vilivyounganishwa: mifumo ya tahadhari ya moto, vidhibiti vya viwandani (SCADA), vifaa vya hospitali na vya matibabu.

Exploit development

Kutoka kwa hitilafu moja ya memory corruption hadi exploit chain kamili yenye remote root access.

Usalama wa browser na web

SOP/CORS bypasses, njia za mashambulizi kwenda kwenye vifaa vya mtandao wa ndani, XSS na usalama wa programu.

Ufichuzi unaowajibika

Kuripoti na kuratibu na wazalishaji na waendeshaji, kutoka kampuni kubwa hadi tawala za miji, pamoja na msaada katika kurekebisha matatizo.

Zana zangu

Tooling na automation kwa vulnerability discovery na penetration testing, pamoja na workflow zinazosaidiwa na AI. Mwandishi wa JavaScript/TypeScript runtime Veloce.

Utafiti

Mwaka	Utafiti / udhaifu	Chanzo
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	rekodi ya CISA katika CIRCL
2013	Apple Motion - CVE-2013-6114 - udhaifu wa usalama	Apple
2014	Apple Web Server - utafiti wa usalama, Februari 2014	Apple
2012	Nokia Hall of Fame - utafiti wa usalama, Desemba 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - moduli ya Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	kumbukumbu ya 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

Mwaka	Utafiti / udhaifu	Chanzo
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

Vyombo vya habari

Mwaka	Makala asili	Chombo cha habari
2025	Ripoti kuhusu responsible disclosure katika Securitas / Marvelit	Security-Insider
2022	Kipindi cha redio kuhusu usalama wa mtandao na udukuzi wa kimaadili	WDR
2024	Majadiliano ya wataalamu wa ÖAG: Usalama 4.0 - usalama wa mtandao na ulinzi kwa AI	medianet (Austria)
2024	Udhaifu wa usalama hospitalini: wagonjwa wako hatarini	Golem
2024	SOP/CORS ya kivinjari na vifaa vya mtandao wa ndani	CYTRES Research
2024	Taarifa ya usalama ya umma kutoka kwa Jean Pereira yenye sasisho lililoandikwa kuhusu marekebisho	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Majadiliano ya wataalamu na Katibu wa Jimbo Tursky kuhusu ujanibishaji wa kidijitali, AI na usalama wa mtandao	KURIER (Austria)
2023	Kushiriki kama mtaalamu wa usalama wa mtandao katika ÖAG Super Tuesday	LEADERSNET (Austria)
2022	Podcast #51: Ethical Hacker - utafiti wa usalama na safari ya kazi	IDG TechTalk / COMPUTERWOCHE
2022	Udhaifu wa usalama wa IT katika jiji la Cologne	Kölner Stadt-Anzeiger
2022	Kamishna wa ulinzi wa data anachunguza udhaifu wa usalama ulioripotiwa lakini ukapuuzwa	WirtschaftsWoche
2022	Responsible disclosure / mashirika 45	Golem
2022	Ripoti kuhusu OBI na mamlaka za umma	connect professional
2020	Hotuba kuu kuhusu usalama wa vivinjari na programu	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: udukuzi wa moja kwa moja wa SCADA/ICS	Hannover Messe / MittelstandsWiki
2019	Mahojiano "Tunahitaji hackers zaidi"	atp magazin
2019	Mashambulizi ya mtandao na darknet - mahojiano na Jean Pereira	Podcast "IT'S IN YOU"
2018	SEO-DAY: jinsi ya kudukua Chrome na kupita SSL mwaka 2018	Host Europe
2018	Hotuba ya usalama katika superpanel ya SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker na mwanzilishi wa SECBIZ kwenye orodha ya wazungumzaji	DSS IT SEC / Riga