Jean Pereira

Έρευνα ασφάλειας · Επιθετική ασφάλεια · Full-stack ανάπτυξη

ΕρευνΩ΄ευπάθειες σε σύνθετα συστήματα και αναπτύσσΩ λογισμικό ασφάλειας και δικά μου προϊόντα για ασφάλεια προγραμμάτΩν περιήγησης, embedded και βιομηχανικά συστήματα, αυτοματοποίηση και AI.

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

Προφίλ

ΒρίσκΩ κενά ασφαλείας εκεί όπου άλλοι σταματούν να ψάχνουν και δημιουργΩ΄ασφαλές λογισμικό που λύνει σύνθετα προβλήματα.

Η δουλειά μου περιλαμβάνει ευπάθειες σε προϊόντα και τεχνολογίες τΩν **Siemens**, **Apple**, **Google**, **Microsoft** και **Nokia**, καθΩς και διάφορα έργα στον τομέα της ιατρικής τεχνολογίας. Αυτή την περίοδο εστιάζΩ στην έρευνα ασφάλειας και τη μηχανική λογισμικού.

Είμαι επίσης δημιουργός του **Veloce**. Μπορείς να επικοινΩνήσεις μαζί μου μέσΩ της φόρμας επικοινΩνίας ή απευθείας στο LinkedIn.

Κύρια σημεία

Τέσσερα **zero-days** στη **Siemens:** συστήματα συναγερμού και ανιχνευτές πυρκαγιάς υπό απομακρυσμένο έλεγχο

Απέκτησα εξ αποστάσεΩς πλήρη έλεγχο συστημάτΩν συναγερμού και ανιχνευτΩν πυρκαγιάς Siemens. Το exploit μου παρείχε πρόσβαση root, τα υψηλότερα δικαιΩματα συστήματος, χΩρίς διαπιστευτήρια, κλικ ή άλλη συμμετοχή του θύματος.

Ανέπτυξα αλυσίδα εκμετάλλευσης τεσσάρΩν άγνΩστΩν ευπαθειΩν και απέδειξα πρακτικά την πλήρη κατάληψη. Επρόκειτο για έλεγχο τεχνολογίας συναγερμού κρίσιμης για την ασφάλεια.

Η Siemens επιβεβαίΩσε τις τέσσερις ανακαλύψεις, CVE-2024-47901, CVE-2024-47902, CVE-2024-47903, CVE-2024-47904. Το exploit έλαβε βαθμολογία CVSS 10.0, η μέγιστη δυνατή κρισιμότητα.

Zero-days σε νοσοκομεία**:** ομάδες αίματος αλλοιΩθηκαν**,** συναγερμοί ΗΚΓ και συσκευές εξαερισμού απενεργοποιήθηκαν

Σε έλεγχο ασφάλειας ανακάλυψα 22 άγνΩστες ευπάθειες σε συσκευές δΩδεκα κατασκευαστΩν και απέδειξα τις επιθέσεις με λειτουργικά exploits: απενεργοποίηση συναγερμΩν ΗΚΓ, διακοπή αερισμού αποστειρΩμένΩν χειρουργείΩν και αλλοίΩση ομάδΩν αίματος και αλλεργιΩν. Ανέπτυξα επίσης παρακάμψεις SOP/CORS για απομακρυσμένες επιθέσεις σε εσΩτερικές συσκευές μη προσβάσιμες απευθείας από το διαδίκτυο.

Οι κατασκευαστές περιλαμβάνουν ZEISS, MOXA, Zebra, Dedalus Labor και Tetronik. ΣύμφΩνα με το ρεπορτάζ Golem του 2024, οι συσκευές χρησιμοποιούνταν σε χιλιάδες άλλα νοσοκομεία και ιατρικές εγκαταστάσεις. Συντόνισα τη γνΩστοποίηση και υποστήριξα τη διόρθΩση. Δημοσιογράφοι παρακολούθησαν όλη τη διαδικασία, από την ενημέρΩση τΩν κατασκευαστΩν έΩς την υποστήριξή μου στις διορθΩσεις.

Ευπάθειες σε περισσότερες από **40** δημόσιες αρχές**,** στην **OBI,** στη **REWE** και στο Ινστιτούτο **Fraunhofer**

Ανακάλυψα ευπάθειες σε 45 δήμους και επιχειρήσεις και τις ανέφερα στους υπευθύνους. Στην OBI, μια ευπάθεια ιστού επέτρεπε κατάληψη συνεδριΩν χρηστΩν και πρόσβαση σε πληροφορίες του εσΩτερικού συστήματος διαχείρισης περιεχομένου.

Πολλοί δήμοι διόρθΩσαν τα προβλήματα. Η OBI απέσυρε τον ιστότοπο μετά τη δημόσια διαμάχη. Τα Golem και WirtschaftsWoche κατέγραψαν την έρευνα και τις αντιδράσεις.

Εμπειρία

Ιουν 2023 - σήμερα

CEO · CTO · CYTRES GmbH

Ίδρυσα και διηύθυνα την εταιρεία με έμφαση στην ανάπτυξη λογισμικού και την έρευνα κυβερνοασφάλειας.

Δεκ 2016 - Αυγ 2019

Εκπαιδευτής κυβερνοασφάλειας · CIC (Cambridge Innovation Center) · Rotterdam, ΚάτΩ ΧΩρες

Πραγματοποίησα εργαστήρια κυβερνοασφάλειας και τεχνική εκπαίδευση.

Δεκ 2016 - Αυγ 2019

Ανώτερος σύμβουλος ασφάλειας · Base Cyber Security · Rotterdam, Κάτω Χώρες

Ηγήθηκα της τεχνικής ομάδας και εκπαίδευσα νέους εργαζομένους μέχρι το απαιτούμενο τεχνικό επίπεδο.

2019

Ιδρυτής · CEO · CTO · Secbiz IT Security GmbH

- Ιδρυτής και τεχνικός επικεφαλής εταιρείας κυβερνοασφάλειας.
- Έρευνα και συμβουλευτική σε βιομηχανική/OT και εφαρμοστική ασφάλεια.
- Ζωντανή επίδειξη επίθεσης SCADA στη Hannover Messe 2019.

Veloce

Το Veloce είναι το δικό μου JavaScript/TypeScript runtime για agentic coding: μια πλατφόρμα-στόχος όπου agents προγραμματισμού μπορούν να δημιουργούν πλήρεις εφαρμογές που είναι ευανάγνωστες, ελέγξιμες και άμεσα εκτελέσιμες, χωρίς να συναρμολογούν πρώτα npm dependencies, frameworks, build tooling και deployment glue.

Το runtime περιλαμβάνει τα βασικά δομικά στοιχεία: περιοριστικό sandbox και μοντέλο permissions, HTTP server, SQLite και PostgreSQL με ORM και KV store, δυνατότητες browser και desktop και packaging σε αυτόνομο native binary. Υπολογιστικά απαιτητικά τμήματα μπορούν να μεταφερθούν από JavaScript/TypeScript σε native kernels βασισμένα σε Rust ή σε WebAssembly. Στόχος είναι λογισμικό που οι agents μπορούν να παράγουν αξιόπιστα, οι άνθρωποι εξακολουθούν να κατανοούν και τα συστήματα εκτελούν με όσο το δυνατόν λιγότερα κινούμενα μέρη.

Εξειδίκευση

Embedded, OT και ιατροτεχνολογικός εξοπλισμός

Έρευνα ευπαθειών σε firmware και συνδεδεμένες συσκευές: συστήματα πυρανίχνευσης, βιομηχανικοί ελεγκτές (SCADA), νοσοκομειακός και ιατρικός εξοπλισμός.

Ανάπτυξη **exploits**

Από μία μεμονωμένη ευπάθεια memory corruption έως πλήρη αλυσίδα exploit με απομακρυσμένη πρόσβαση root.

Ασφάλεια **browser** και **web**

Παρακάμψεις SOP/CORS, διαδρομές επίθεσης προς συσκευές σε εσωτερικά δίκτυα, XSS και ασφάλεια εφαρμογών.

Υπεύθυνη γνωστοποίηση

Αναφορά και συντονισμός με κατασκευαστές και διαχειριστές, από μεγάλες εταιρείες έως δημοτικές αρχές, συμπεριλαμβανομένης της υποστήριξης αποκατάστασης.

Δικά μου εργαλεία

Εργαλεία και αυτοματοποίηση για εντοπισμό ευπαθειών και penetration testing, συμπεριλαμβανομένων workflow με υποστήριξη AI. Δημιουργός του JavaScript/TypeScript runtime Veloce.

Έρευνα

Έτος	Έρευνα / ευπάθεια	Πηγή
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	καταχώριση CISA στο CIRCL
2013	Apple Motion - CVE-2013-6114 - ευπάθεια	Apple
2014	Apple Web Server - έρευνα ασφάλειας, Φεβρουάριος 2014	Apple
2012	Nokia Hall of Fame - έρευνα ασφάλειας, Δεκέμβριος 2012	Nokia
2012	Android Browser DoS - CVE-2012-6301 - μονάδα Metasploit	Rapid7
2012	Microsoft Excel - CVE-2012-5672 - Memory Corruption / Denial of Service	αρχείο 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

Έτος	Έρευνα / ευπάθεια	Πηγή
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

Τύπος

Έτος	Αρχικό άρθρο	Μέσο
2025	Κάλυψη της υπεύθυνης γνΩστοποίησης στη Securitas / Marvelit	Security-Insider
2022	ΡαδιοφΩνικό αφιέρΩμα για την κυβερνοασφάλεια και το ηθικό hacking	WDR
2024	Συζήτηση ειδικΩν της ÖAG: Ασφάλεια 4.0 - κυβερνοασφάλεια και άμυνα με ΤΝ	medianet (Αυστρία)
2024	Ευπάθειες ασφαλείας σε νοσοκομεία: ασθενείς σε κίνδυνο	Golem
2024	SOP/CORS του προγράμματος περιήγησης και συσκευές εσΩτερικού δικτύου	CYTRES Research
2024	Δημόσια ειδοποίηση ασφαλείας του Jean Pereira με τεκμηριΩμένη ενημέρΩση αποκατάστασης	Volksbank / Sparda Bank (Responsible Disclosure)
2023	Συζήτηση με τον υφυπουργό Tursky για την ψηφιοποίηση, την ΤΝ και την κυβερνοασφάλεια	KURIER (Αυστρία)
2023	Συμμετοχή Ως ειδικός κυβερνοασφάλειας στο ÖAG Super Tuesday	LEADERSNET (Αυστρία)
2022	Podcast #51: Ethical Hacker - έρευνα ασφάλειας και επαγγελματική πορεία	IDG TechTalk / COMPUTERWOCHE
2022	Ευπάθεια ασφάλειας ΤΠ στον Δήμο της ΚολΩνίας	Kölner Stadt-Anzeiger
2022	Η επίτροπος προστασίας δεδομένΩν ερευνά αναφερθείσα ευπάθεια ασφαλείας που αγνοήθηκε	WirtschaftsWoche
2022	Υπεύθυνη γνΩστοποίηση / 45 οργανισμοί	Golem
2022	Ρεπορτάζ για την OBI και δημόσιες αρχές	connect professional
2020	Keynote για την ασφάλεια προγραμμάτΩν περιήγησης και εφαρμογΩν	OMT - Online Marketing Konferenz
2019	Industrial Security Forum: ζΩντανό hacking SCADA/ICS	Hannover Messe / MittelstandsWiki
2019	Συνέντευξη «Χρειαζόμαστε περισσότερους hackers»	atp magazin
2019	Κυβερνοεπιθέσεις & darknet - συνέντευξη με τον Jean Pereira	Podcast "IT'S IN YOU"
2018	SEO-DAY: πΩς να χακάρετε το Chrome και να παρακάμψετε το SSL το 2018	Host Europe
2018	Ομιλία ασφάλειας στο superpanel του SEO-DAY 2018	SEO-DAY / Online-Profession
2018	International Cyber Security Conference: Ethical Hacker και ιδρυτής της SECBIZ στη λίστα ομιλητΩν	DSS IT SEC / Riga