TEAM82 DI CLAROTY RIVELA CHE IL 63% DELLE VULNERABILITÀ NOTE MONITORATE DAL CISA SONO LEGATE ALLE RETI DI AZIENDE SANITARIE.

Lo "State of CPS Security Report: Healthcare 2023" di Claroty riporta le sorprendenti lacune presenti nella sicurezza dei dispositivi medici direttamente collegati alla cura del paziente.

Milano, 12 marzo 2024 – Claroty, azienda specializzata nella protezione dei sistemi cyber-fisici, ha presentato, nel corso della conferenza annuale HIMSS24, un nuovo rapporto relativo alla sicurezza dei dispositivi medici collegati alle reti di organizzazioni sanitarie, come ospedali e cliniche. Lo "State of CPS Security Report: Healthcare 2023" riporta dati sconcertanti: il 63% delle vulnerabilità sfruttate note (KEV) monitorate da CISA sono legate alle reti sanitarie e il 23% dei dispositivi medici, inclusi dispositivi di imaging, dispositivi di IoT clinici e dispositivi chirurgici, presenta almeno un KEV.

Nella prima edizione dello "State of CPS Security Report" dedicata al settore sanitario, Team82, il pluripremiato gruppo di ricercatori Claroty, ha analizzato come dispositivi medici e sistemi di assistenza al paziente sempre più connessi aumentino esponenzialmente il rischio di attacchi informatici mirati ad interrompere i servizi ospedalieri. Lo scopo di questa ricerca è dimostrare l'aumento della connettività dei dispositivi medici critici, dai sistemi di imaging alle pompe per infusione, e descrivere le implicazioni legate alla loro crescente esposizione online. Vulnerabilità e debolezze di implementazione emergono spesso nella ricerca di Team82 e in ciascuno di questi casi è possibile tracciare una linea diretta con esiti potenzialmente negativi per i pazienti.

"*La connettività ha portato grandi cambiamenti all'interno delle reti ospedaliere con notevoli miglioramenti nella cura dei pazienti, permettendo ai medici di diagnosticare, prescrivere e trattare a distanza, con un'efficienza mai vista prima*" ha affermato **Amir Preminger, Vice President of Research di Claroty**. "*Tuttavia, l'aumento della connettività richiede un'architettura di rete adeguata e una maggiore consapevolezza dell'esposizione ai rischi ad essa legati. Le aziende sanitarie e i loro security partner devono sviluppare politiche e strategie che prevedano dispositivi e sistemi medici resilienti, in grado di resistere alle intrusioni. Ciò include l'accesso remoto sicuro, la definizione delle priorità nella gestione del rischio e l'implementazione della segmentazione*".

Di seguito, i risultati chiave contenuti nel Report:

- **Esposizione delle reti guest**: il 22% degli ospedali dispone di dispositivi che collegano le reti guest, che forniscono a pazienti e visitatori l'accesso WiFi, e le reti interne. Questo rappresenta un vettore di attacco molto pericoloso, in quanto un utente malintenzionato può trovare e prendere rapidamente di mira le risorse presenti sul WiFi pubblico e sfruttare tale accesso come ponte verso le reti interne, sulle quali risiedono i dispositivi per la cura dei pazienti. Dato ancora più allarmante, evidenziato dalla ricerca di Team82:il 4% dei dispositivi chirurgici – apparecchiature critiche che in caso di malfunzionamento potrebbero avere un impatto negativo sulla cura del paziente – comunica tramite le reti guest.

- **Sistemi operativi non supportati o al termine del ciclo di vita**: il 14% dei dispositivi medici connessi utilizza sistemi operativi non supportati o al termine del ciclo di vita. Dei dispositivi non supportati, il 32% sono dispositivi di imaging, compresi i sistemi a raggi X e MRI, che sono vitali per la diagnosi e il trattamento prescrittivo, e il 7% sono dispositivi chirurgici.

- **Elevata probabilità di sfruttamento**: il rapporto ha esaminato i dispositivi con punteggi EPSS (Exploit Prediction Scoring System) elevati, che si riferiscono alla probabilità che una vulnerabilità del software venga sfruttata per potenziali attacchi su una scala da 0 a 100. L'analisi ha mostrato che l'11% dei dispositivi dei pazienti, come le pompe per infusione, e il 10% dei dispositivi chirurgici presentano vulnerabilità con punteggi EPSS elevati. Un'analisi più profonda ha rivelato, inoltre, che quando si prendono in considerazione apparecchiature con sistemi operativi non supportati, l'85% dei dispositivi chirurgici in quella categoria ha punteggi EPSS elevati.

- **Dispositivi accessibili da remoto**: la ricerca ha esaminato anche quali dispositivi medici sono accessibili da remoto e ha scoperto che molti di quelli che, in caso di guasto, provocano elevate conseguenze per i pazienti, inclusi defibrillatori, sistemi di chirurgia robotica e gateway di defibrillatori, rientrano in questa categoria. Team82 ha, inoltre, rivelato che il 66% dei dispositivi di imaging, il 54% dei dispositivi chirurgici e il 40% dei dispositivi di assistenza diretta sono accessibili da remoto.

Per consultare i risultati completi della ricerca, le analisi approfondite e le misure di sicurezza consigliate da Team82 in risposta alle vulnerabilità è possibile scaricare lo "State of CPS Security Report: Healthcare 2023".

Methodology

The State of CPS Security Report: Healthcare 2023 is a snapshot of healthcare cybersecurity trends, medical device vulnerabilities, and incidents observed and analyzed by Team82, Claroty's threat research team, and our data scientists. Information and insights from trusted open sources, including the National Vulnerability Database (NVD), the Cybersecurity and Infrastructure Security Agency (CISA), the Healthcare Sector Coordinating Council Working Group, and others, also were used to bring invaluable context to our findings.

Acknowledgements

The primary author of this report is Chen Fradkin, full stack data scientist at Claroty. Contributors include: Ty Greenhalgh, industry principal healthcare, Yuval Halaban, risk team lead, Rotem Mesika, threat and risk group lead, Nadav Erez, vice president of data and Amir Preminger, vice president of research. Special thanks to the entirety of Team82 and the data department for providing exceptional support to various aspects of this report and research efforts that fueled it.

Claroty

Claroty è specializzata in soluzioni di sicurezza volte a proteggere i sistemi cyber-fisici in ambienti industriali (OT), sanitari (IoMT) e aziendali (IoT): il cosiddetto Extended Internet of Things (XIoT). La piattaforma unificata dell'azienda si integra con l'infrastruttura esistente dei clienti per fornire una gamma completa di controlli per la visibilità, la gestione dei rischi e delle vulnerabilità, il rilevamento delle minacce e un accesso sicuro da remoto. Supportate dalle più grandi società di investimento e provider di automazione industriale del mondo, le soluzioni Claroty vengono distribuite da centinaia di organizzazioni in migliaia di siti in tutto il mondo. La società ha sede a New York e filiali in Europa, Asia-Pacifico e America Latina. Per maggiori informazioni: www.claroty.com

Ufficio Stampa

Meridian Communications Srl

Via Cuneo, 3 – 20149 Milano Tel. +39 02 48519553

Silvia Ceriotti	335 7799816	silvia.ceriotti@meridiancommunications.it
Viviana Bandieramonte	329 4776937	viviana.bandieramonte@meridiancommunications.it
Ilaria Malgrati	339 2143042	ilaria.malgrati@meridiancommunications.it