VEDERE LABS

Esposizione online dei sistemi e dispositivi medici

Sottotitolo

26 settembre 2022

1. Sintesi

Il 12 settembre l'FBI ha pubblicato una segnalazione per il settore privato intitolata "I dispositivi medici senza patch e obsoleti offrono opportunità di attacchi informatici" e incentrata sul fatto che un numero crescente di vulnerabilità nei dispositivi medici può venire sfruttata da attori di minacce per "compromettere le funzioni operative, la sicurezza dei pazienti, la riservatezza dei dati e l'integrità degli stessi nelle strutture sanitarie".

La segnalazione giunge dopo la scoperta di vulnerabilità significative, nel corso di quest'anno, che riguardano dispositivi medici come pompe infusionali, sistemi di erogazione dei farmaci ed elettrocardiografi, oltre a un'ondata di attacchi ransomware mirati alle organizzazioni sanitarie negli anni scorsi, alcuni dei quali hanno reso i dispositivi medici inutilizzabili.

In questo report tratteremo i motivi per i quali i dispositivi medici risultano vulnerabili, andando oltre le vulnerabilità per fornire un quadro dell'esposizione dei sistemi e dei dispositivi medici nell'Internet aperta, ed esamineremo le raccomandazioni di mitigazione dei rischi per le organizzazioni sanitarie.

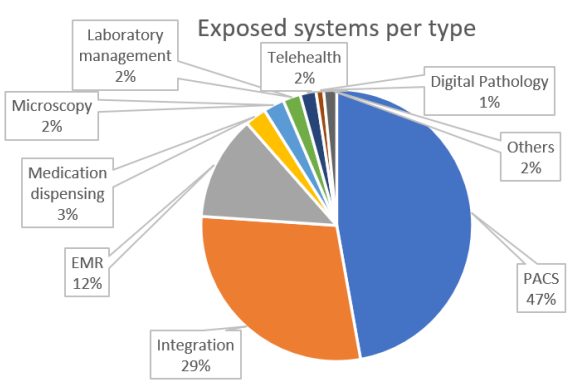
Le conclusioni principali includono:

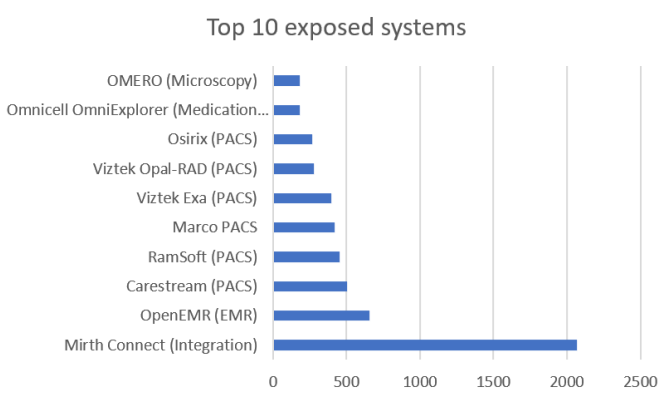
- Troviamo oltre 7000 sistemi medicali esposti online, tra cui PACS, motori di integrazione sanitaria, EMR, sistemi di erogazione dei farmaci, eccetera. Alcuni dispositivi medici, come le stampanti per immagini medicali, risultano inoltre esposti direttamente.
- Gli Stati Uniti contano la grande maggioranza dei sistemi esposti (il 58% del totale), seguiti da Iran, India e Brasile.
- Quasi la metà dei sistemi esposti sono PACS che generalmente si affidano al protocollo DICOM per la memorizzazione e il recupero delle immagini medicali. Esaminando specificamente i sistemi DICOM, notiamo 4114 sistemi esposti, un aumento del 14% rispetto a un anno fa.
- L'applicazione di un'efficace segmentazione di rete rappresenta l'azione mitigatrice più importante, considerate le nostre conclusioni sui sistemi esposti.

2. Analisi dei sistemi medicali esposti online

Tramite una serie di specifiche impronte di rete dei sistemi medicali (accessibili apertamente a chiunque, inclusi gli aggressori), abbiamo posto una query sul motore di ricerca Shodan e scoperto un totale di 7168 sistemi esposti. Più di tre quarti dei sistemi si trovano nelle Americhe, con i soli Stati Uniti ad averne 4185 (il 58% del totale). La regione Asia-Pacifico con il Giappone (APJ) è seconda, rappresentata soprattutto da India (324 sistemi esposti) e Australia (146). La terza è l'Europa, con la maggior parte dei sistemi esposti in Germania (128), Regno Unito (75) e Paesi Bassi (71). Infine, nella regione META (Medio Oriente, Turchia e Africa), il paese più rappresentativo risulta l'Iran, con 427 sistemi esposti.

I sistemi esposti si suddividono nei seguenti tipi.





Quasi la metà sono PACS, utilizzati per la memorizzazione e la visualizzazione delle immagini medicali in base al protocollo standard DICOM. La seconda categoria più popolare sono i motori di integrazione sanitaria, utilizzati per standardizzare i flussi dei dati tra sistemi separati come i dati clinici, finanziari e operativi. Questi motori utilizzano spesso il protocollo standard HL7. La terza categoria sono i sistemi dei record medicali elettronici (EMR), utilizzati per gestire i dati sanitari dei pazienti. Una categoria interessante e sorprendente nelle prime 10 è rappresentata dai sistemi di erogazione dei farmaci, utilizzati in genere nelle farmacie degli ospedali.

Esaminando soltanto i primi 10 sistemi esposti, abbiamo scoperto che 882 su 5405 (16%) hanno almeno una vulnerabilità individuata da Shodan. Per alcuni sistemi l'indice di vulnerabilità risultava molto più alto. Per Opal-RAD PACS è del 69%, per Carestream PACS del 50% e per OpenEMR del 31%. Vale inoltre la pena di notare che molti altri sistemi potrebbero presentare vulnerabilità non individuate automaticamente dal motore di ricerca.

Poiché i PACS sono il tipo più comune di sistema esposto, abbiamo deciso di esaminarli più da vicino. Come menzionato più sopra, i sistemi PACS si servono generalmente del protocollo DICOM, così abbiamo ampliato la ricerca per trovare altri sistemi esposti tramite la query "Risposta del server DICOM", che ha prodotto 4114 risultati. I dispositivi che utilizzano DICOM espongono il nome (o un identificativo) dell'applicazione del server sul banner raccolto da Shodan. Uno dei server più popolari trovati online utilizza il toolkit OFFIS DICOM di cui a giugno è stato divulgato un insieme di vulnerabilità.

3. Raccomandazioni per la mitigazione dei rischi

La segnalazione dell'FBI propone cinque categorie di azioni mitigatrici per i dispositivi medici vulnerabili:

- Eseguire la protezione degli endpoint come antivirus ed EDR sui dispositivi che supportano quelle tecnologie.
- Utilizzare password uniche complesse per ciascun dispositivo e limitare il numero dei tentativi di login.
- Mantenere un inventario dei dispositivi medici e utilizzarlo per la valutazione dei rischi.
- Seguire gli avvisi di sicurezza dei fornitori ed eseguire la scansione delle vulnerabilità sui dispositivi medici.
- Avviare la formazione alla sicurezza rivolta ai dipendenti per individuare e segnalare problemi come le minacce interne, il phishing e l'ingegneria sociale.

La segnalazione incoraggia inoltre ad "adottare altre precauzioni mitigatrici come l'isolamento del dispositivo dalla rete o l'audit delle attività di rete del dispositivo". Per linee guida più dettagliate sull'attuazione della segmentazione per tipi specifici di dispositivi come PACS, EMR e pompe infusionali, vedi le pubblicazioni di orientamento alla sicurezza NIST. Per un orientamento generale sulla valutazione dei rischi dei dispositivi medici vedi il recente NIST SP 800-66.

La segmentazione della rete risulta estremamente importante, considerate le nostre conclusioni sui sistemi esposti. Le raccomandazioni dell'FBI, in particolare la segmentazione e il monitoraggio della rete, dovranno venir applicate non solo ai dispositivi medici, ma a ciascun dispositivo nella rete della propria organizzazione. Come abbiamo spiegato nei post precedenti, e come trattato di recente dal Centro per la Coordinazione della Sicurezza Informatica nel Settore Sanitario (HC3), gli attori di minacce possono usare a proprio vantaggio altri tipi di dispositivi per ottenere l'accesso o compromettere le organizzazioni sanitarie.

Per maggiori informazioni e analisi tecniche, si prega di leggere l'intero report in questo link.