VEDERE LABS

Gefährdung von medizinischen Geräten und Systemen im

Zwischentitel

26. September 2022

1. Zusammenfassung

Am 12. September veröffentlichte das FBI eine an die Privatwirtschaft adressierte Mitteilung mit dem Titel „Nicht aktualisierte und veraltete medizinische Geräte als Einfallstor für Cyberattacken“. Gegenstand der Mitteilung war, dass böswillige Akteure immer mehr Schwachstellen in medizinischen Geräten ausnutzen können, um die „operative Funktionalität von Gesundheitseinrichtungen, Patientensicherheit, Datenschutz und Datenintegrität zu beeinträchtigen“.

Diese Mitteilung folgt auf die diesjährige Entdeckung erheblicher Schwachstellen in medizinischen Geräten wie Infusionspumpen, Dosiersystemen für Medikamente und Elektrokardiographen sowie auf eine Welle von Ransomware-Attacken gegen Gesundheitseinrichtungen in den letzten Jahren, die teilweise dazu führten, dass medizinische Geräte nicht mehr genutzt werden konnten.

In diesem Bericht erläutern wir, warum medizinische Geräte verwundbar sind, blicken über die Schwachstellen hinaus, um aufzuzeigen, wie exponiert medizinische Geräte und Systeme im offenen Internet sind, und empfehlen Gegenmaßnahmen, die Gesundheitseinrichtungen ergreifen können.

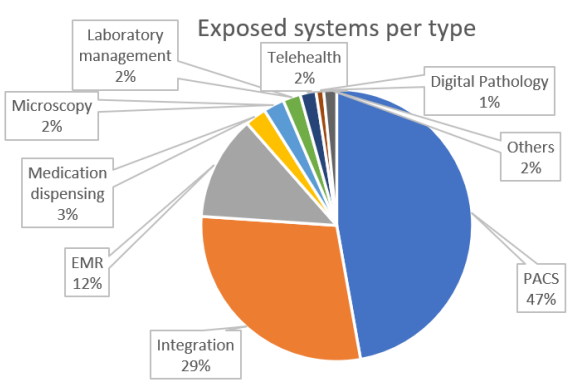
Die wichtigsten Erkenntnissen dieses Berichts sind:

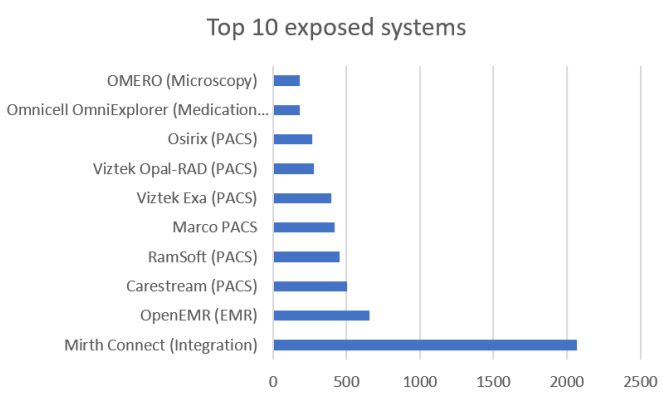
- Wir haben über 7.000 gefährdete medizinische Geräte im Internet gefunden, unter anderem PACS, Integration Engines für das Gesundheitswesen, EMR, Dosiersysteme für Medikamente und viele weitere. Diverse medizinische Geräte wie Drucker für medizinische Bilder sind direkt gefährdet.
- Die meisten der gefährdeten Systeme befanden sich in den USA (insgesamt 58 %), gefolgt vom Iran, Indien und Brasilien.
- Bei fast der Hälfte der gefährdeten Systeme handelt es sich um PACS, die für Speicherung und Abruf medizinischer Bilder in der Regel das DICOM-Protokoll nutzen. Insbesondere bei DICOM-Systemen haben wir 4.114 gefährdete Systeme gefunden, was einer Steigerung von 14 % innerhalb eines Jahres entspricht.
- Unter Berücksichtigung unserer Erkenntnisse zu exponierten Systemen erachten wir eine effektive Netzwerksegmentierung als wirksamste Gegenmaßnahme.

2. Eine Analyse gefährdeter medizinischer Systeme im Internet

Unter Verwendung spezifischer Netzwerk-Fingerabdrücke von medizinischen Systemen (die für alle sichtbar sind, auch für Angreifer), haben wir eine Abfrage mit der Suchmaschine Shodan durchgeführt und insgesamt 7.168 exponierte Systeme gefunden. Mehr als drei Viertel der Systeme befinden sich auf dem amerikanischen Kontinent, davon allein 4.185 (insgesamt 58 %) in den USA. Die Region Asien/Pazifik und Japan (APJ) steht an zweiter Stelle, wobei Indien mit 324 und Australien mit 146 exponierten Systemen die meisten Schwachstellen aufweisen. Europa folgt an dritter Stelle; hier befinden sich die meisten exponierten Systeme in Deutschland (128), im Vereinigten Königreich (75) und in den Niederlanden (71). An letzter Stelle steht die Region Mittlerer Osten, Türkei und Afrika (META), wo Iran mit 427 die meisten exponierten Systeme aufweist.

Die exponierten Systeme lassen sich in die folgenden Kategorien unterteilen.





Fast die Hälfte sind PACS, die zum Speichern und Abrufen medizinischer Bilder genutzt werden, wobei standardmäßig das DICOM-Protokoll zum Einsatz kommt. An zweiter Stelle stehen Integration Engines für das Gesundheitswesen, die zur Angleichung von Datenströmen aus unter anderem klinischen, finanziellen und operativen Daten auf separaten Systemen verwendet werden. Diese Engines nutzen oft standardmäßig das HL7-Protokoll. Bei der dritten Kategorie handelt es sich um Systeme für elektronische Krankenakten (Electronic Medical Records, EMR), die zur Verwaltung von Patientendaten verwendet werden. Interessanter- und überraschenderweise ist in den Top 10 auch die Kategorie Dosiersysteme für Medikamente vertreten, die in der Regel in Krankenhausapotheken zum Einsatz kommen.

Blicken wir nur auf die Top 10 der exponierten Systeme, zeigt sich, dass 882 von 5.405 Geräten (16 %) mindestens eine Schwachstelle aufwiesen, die von Shodan identifiziert wurde. Bei manchen Systemen war die Anfälligkeitsrate wesentlich höher. Bei Opal-RAD PACS betrug sie 69 %, bei Carestream PACS 50 % und bei OpenEMR 31 %. Ferner ist anzumerken, dass viele weitere Systeme Schwachstellen haben könnten, die nicht automatisch von der Suchmaschine identifiziert werden.

Da PACS die Spitzenposition bei den exponierten Systeme einnehmen, wollten wir uns genauer mit diesen Systemen befassen. Wie oben erwähnt, nutzen PACS in der Regel das DICOM-Protokoll, sodass wir unsere Suche um den Suchbegriff „DICOM Server Response“ erweitert haben, was zu 4.114 neuen Ergebnissen führte. Geräte, die DICOM nutzen, geben den Namen (oder ein Identifizierungsmerkmal) der Serveranwendung auf dem Banner preis, das Shodan abruft. Einer der beliebtesten Server, den wir online gefunden haben, verwendet das OFFIS DICOM Toolkit, bei dem erst im Juni diverse Schwachstellen entdeckt wurden.

3. Empfohlene Gegenmaßnahmen

In der Mitteilung des FBI werden fünf Kategorien von Gegenmaßnahmen für gefährdete medizinische Geräte vorgeschlagen:

- Nutzen Sie einen Endpunktschutz wie Antivirensoftware und EDR für Geräte, die solche Technologien unterstützen.
- Verwenden Sie komplexe, individuelle Passwörter für jedes Gerät und schränken Sie die Anzahl der Anmeldeversuche ein.
- Erfassen Sie alle medizinischen Geräte in einer Inventarliste, um eine Risikobewertung durchzuführen.
- Befolgen Sie die Sicherheitsempfehlungen der Anbieter und überprüfen Sie medizinische Geräte auf Schwachstellen.
- Bieten Sie Sicherheitsschulungen für Beschäftigte an, damit sie in der Lage sind, Probleme wie interne Bedrohungen, Phishing und Social Engineering zu erkennen und zu melden.

In der Mitteilung wird außerdem empfohlen, „weitere Vorsichtsmaßnahmen zu ergreifen, zum Beispiel das Gerät vom Netzwerk zu trennen oder die Netzwerkaktivitäten des Geräts zu überprüfen“. Die Sicherheitsbulletins des NIST enthalten ausführlichere Richtlinien zur Segmentierung spezifischer Gerätetypen wie PACS, EMR und Infusionspumpen. Allgemeine Hinweise zur Risikobewertung von medizinischen Geräten finden sich im aktuellen Bulletin NIST SP 800-66.

Eine Netzwerksegmentierung wird angesichts unserer Erkenntnisse über exponierte Systeme dringend empfohlen. Die Empfehlungen des FBI, insbesondere zur Segmentierung und Überwachung von Netzwerken, sollten nicht nur für medizinische Geräte, sondern für alle Geräte im Netzwerk Ihrer Organisation umgesetzt werden. Wie unsere früheren Analysen und die aktuelle Diskussion des Health Sector Cybersecurity Coordination Center (HC3) zeigen, können böswillige Akteure diese weiteren Gerätetypen nutzen, um sich Zugang zu verschaffen zu Gesundheitseinrichtungen oder ihnen zu schaden.

Weitere Informationen und technische Analysen finden Sie im vollständigen Bericht.