aplite

Tailor-made IT Security

Securing Healthcare Data: Modernizing DICOM Protocol

Ibrahim Akkulak <ibrahim@aplite.de>

Aplite GmbH – Formed With a Mission To Help Organizations Enhancing Their IT Security

Who we are

We're a collective group of IT security experts providing top-notch services to help organizations address the most pressing IT security challenges.

Sina Yazdanmehr

Co-founder & Managing Director

- **Co-Founder** Aplite GmbH | Now
- **Team Lead** at SRLabs | 2022-2023
- **Sr. IT Security Consultant** at SRLabs | 2020-2023
- **IT Security Consultant** at SRLabs | 2018-2020
- **Pentester** at Infigo IS | 2016-2018
- **Pentester** at IUT Cert | 2010-2015

Ibrahim Akkulak

Co-founder & Managing Director

- **Co-Founder** Aplite GmbH | Now
- **Founder** at Ibency | 2018
- **Cloud Security Consultant** at Accenture| 2021-2022
- **IT Security Consultant** at Cloudyrion | 2020-2021
- **Developer** at Siemens | 2018-2020

What do we do

- **Security Risk Assessment.** Assess and secure (Cloud/legacy) infrastructure and applications.
- **Secure by Design.** Secure your infra/app designs from scratch.
- **Security Strategy & Roadmap Advisory.** Tailor a security program fitting your organization.
- **Security Architecture Review.** Pinpoint architectural security gaps and collaboratively enhance them.

How we do it

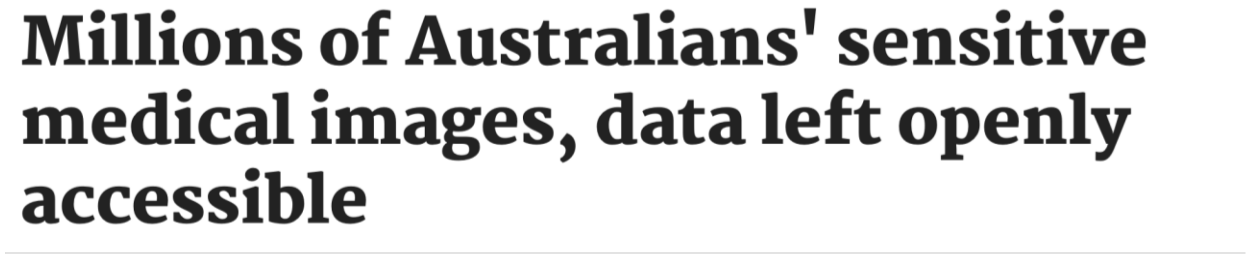
We don't just hand you a report and walk away! We tailor security measures to your unique needs after a comprehensive assessment, effectively communicate with all levels of your organization, and actively guide the implementation process for robust security. We ensure that our approach aligns perfectly with your business goals.

Medical Imaging Systems Have Been a Known Source of Sensitive Data Leakage

Some security researchers have also investigated this issue and shared some findings

2019,

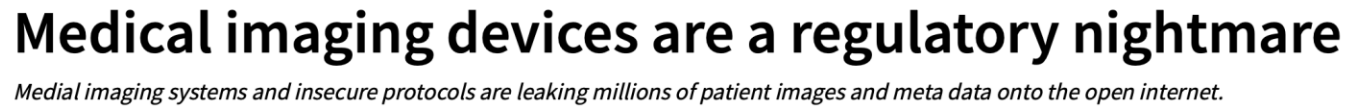
iTnews Australia [1]



Millions of Australians' sensitive medical images, data left openly accessible

2021,

CybelAngel [2]



Medical imaging devices are a regulatory nightmare

Medial imaging systems and insecure protocols are leaking millions of patient images and meta data onto the open internet.

1. https://itnews.com.au/news/millions-of-australians-sensitive-medical-images-data-left-openly-accessible-531248
2. https://cybelangel.com/stop-medical-device-leaks/

2023 Update: The Threat Is Growing Globally With More Leaked Sensitive Data

Our Internet-wide research shows **3,806** medical imaging servers are accessible, **1,129** of which leak **over 59M** sensitive patients' records

Type of Data	Count	Description
Personal Identifiable Information (PII)	> 16M	Personal data containing information like **full name, address, birthdate, gender, patient's ID, in some cases SSN, etc.**
Protected Health Information (PHI)	> 43M	Medical records containing information such as **patient's full name, results and date of examination, patient's ID, etc.**

- The servers are hosted in **111 different countries**
- A server may store patients' data from other countries

Root Cause: DICOM, the standard protocol in medical imaging, lacks an adequate access control mechanism

- Medical imaging encompasses a range of techniques such as X-Rays, CT scans, and MRIs, used to visualize internal body structures, with DICOM serving as the standard protocol for storing and transmitting these images
- The security problems with DICOM are connected to using legacy protocols on the internet as industries strive to align with the transition towards Cloud-based solutions
- Built-in access control in the standard is inadequate because it's optional, disabled by default, relies on a 16-byte Application Entity Title (AET), lacks rate limits, and doesn't offer a credential provisioning method for medical modalities

Aplite Has Initiated an Extensive Project in Partnership with Bochum Economic Development Center and Bochum HealthCampus to Improve DICOM Security

We are committed to enhancing the privacy of personal and medical data for individuals worldwide through the improvement of DICOM security

Increase awareness

- We have been conducting a comprehensive internet-wide research on DICOM since early this year
- We have initiated our collaboration with the DICOM standard organization to issue an advisory for vendors
- We will present all the research's findings, along with technical details, at BlackHat EU in December [3]

Research and development project

- We have initiated a research and development project, in collaboration with Bochum economic center, to enhance DICOM security
- This is an incredible journey filled with challenges. Together, we can overcome these challenges and achieve our mission of helping people worldwide. **Join us as we embark on this global mission!**

[3] https://www.blackhat.com/eu-23/briefings/schedule/index.html#millions-of-patient-records-at-risk-the-perils-of-legacy-protocols-34188

Takeaways

1. Over 59M patients’ records including sensitive data are accessible on the internet
2. DICOM insufficient access control mechanism is the root cause of this leakage
3. We aim to enhance DICOM security and address this issue via a R&D project

Thank you!

Aplite GmbH | Tailor-made IT Security

Web: www.aplite.de
Email: hi@aplite.de