DICOM Security Advisory

Version 1

November 1, 2023

Author: Sina Yazdanmehr <sina@aplite.de>

Introduction

In the realm of DICOM storage and access, two common network setups are prevalent:

- **Remotely hosted.** Hosting DICOM storage on the internet, e.g., on the Cloud. This involves exposing DICOM to the internet, allowing modalities within a medical institution to upload examination results, and enables medical staff to access the data remotely.
- **On-Premises.** Typically hosted within a medical institution's own infrastructure. The server may be exposed to facilitate access by other institutions remotely.

In both cases, it is important to recognize that remote exposure carries the inherent risk of potential data leakage.

Additionally, DICOM is at risk of network attacks, such as Man-In-The-Middle, within internal networks.

Mitigation Recommendations

There are several solutions that each medical institution can implement to harden their setup.

Before considering the implementation of these solutions, it is essential to evaluate whether there is a genuine need to expose the DICOM server to remote access. If remote access is unnecessary, it is advisable to keep it internal.

Additionally, each DICOM setup may vary, and the suitability of these solutions can differ accordingly. Therefore, it is highly recommended to consult with an expert before implementing any of these solutions.

- **Point-to-multipoint setup.** DICOM storage hosted either remotely or on-premises, accessible to multiple remote users. In this case:
    - **Enable the extended negotiation of user identity, if applicable.** Enable the feature If the DICOM storage application and the client applications support it. For enhanced security, integrate it with an IAM backend to establish a robust authentication and authorization mechanism. In case where IAM integration is not feasible, consider using *User-Identity-Type*[1] 2 along with unique and strong credentials for each user. Ensure that no unauthenticated request is permitted.
    - **Source IP address whitelisting.** Configuring source IP address whitelisting for the DICOM server, permitting access only from the medical institution’s static public IP address. This feature is widely supported by most DICOM implementations.

[1] https://dicom.nema.org/medical/dicom/current/output/chtml/part07/sect_D.3.3.7.html#table_D.3-14

Additionally, whitelisting can be applied by a firewall. If serving users without static public IP addresses, consider implementing a streaming reverse proxy[2] with applied authentication. Please note that the stream reverse proxy is a workaround and not a standard solution; it may introduce errors and lead to functionality issues.

- **Site-to-site setup.** DICOM storage hosted remotely, for example on a Cloud infrastructure, accessible exclusively through the medical institution's internal network by modalities and medical staff. In this case:
    - **Establish a secure channel.** Create a secure site-to-site channel[3], such as IPSec tunnel[4], between the DICOM server and the internal network. Ensure the DICOM server is accessible only via this secure channel, and data exchanged is encrypted. Since DICOM implementations often lack built-in support for this type of channel, additional termination points[5] may be necessary.
    - **Source IP address whitelisting.** If establishing a secure channel is not feasible, consider source IP whitelisting as mentioned above.

  For enhanced security, consider using the extended negotiation of user identity as mentioned above.

In any of these cases consider enabling Application Entity Title (AET) whitelisting on association level[6], if applicable.

Additionally, for enhanced security consider:

- **TLS connection.** If modalities and software in use in a network support TLS, it is highly recommended to enable TLS.
- **Network segmentation and segmentation.** It is imperative to implement robust network policies within the internal network to effectively isolate DICOM communications from the rest of the network. Ensure that only authorized individuals and systems who require access have permission to this segment.
- **Monitoring.** Implement proper logging on your DICOM systems and establish network monitoring to be able to detect and respond to potential attacks promptly.

[2] https://nginx.org/en/docs/stream/ngx_stream_proxy_module.html
[3] https://en.wikipedia.org/wiki/Virtual_private_network
[4] https://en.wikipedia.org/wiki/IPsec
[5] https://nstec.com/what-is-vpn-termination-point/
[6] https://dicom.nema.org/dicom/2013/output/chtml/part07/sect_D.3.html