DICOM®

Digital Imaging and Communications in Medicine

ITEM: DICOM FAQ Response to 128-byte preamble vulnerability

DATE: May 2019

This document addresses a reported vulnerability in the preamble defined by the DICOM File format. The vulnerability could allow DICOM files stored on media to have executable malware inserted. The DICOM Network Communications protocol between modalities, PACS, and display systems does not transmit a preamble and is not subject to this vulnerability.

The DICOM security workgroup welcomes efforts to strengthen systems against cybersecurity attacks, to raise awareness of potential attack vectors, and to help users and developers understand how to guard against them.

Background:

DICOM files on media like CDs and DVDs include a 128-byte preamble at the start of the file. The 4 bytes following the preamble contain the characters "DICM" to indicate the body of the file contains DICOM information.

The intended purpose of the preamble is to allow both DICOM software and non-DICOM software to process the same file. A DICOM viewer, for example, will ignore the preamble, observe the DICM string, process the DICOM content, and display the DICOM images. A TIFF viewer could use offset information in the preamble to access and display the image pixel arrays in the file while ignoring the rest of the DICOM content.

A recent article by DICOM editor David Clunie describes using this feature to facilitate a transition in Pathology whole slide imaging from TIFF to DICOM. http://www.jpathinformatics.org/text.asp?2019/10/1/12/255397

When the feature is not being used, all 128 bytes in the preamble are set to 00H. See DICOM Part 10, Section 7.1 http://dicom.nema.org/medical/dicom/current/output/chtml/part10/chapter_7.html#sect_7.1.

DICOM network transmissions (C-Store, C-Move) do not include this preamble. If images imported from media contain a preamble, it is stripped off before being sent. Some DICOM receivers add an empty preamble when they receive and locally store the images.

Description of Vulnerability:

The potential exists to abuse the 128-byte preamble. A malicious actor could modify a DICOM file so that it is treated as both an executable program and as a DICOM file. A user might be somehow convinced to execute the file.

Alternatively, a separate malicious actor, that knew about the embedded executable and had access to the modified file, could be installed and executed to trigger the malware. This type of intrusion is referred to as a multi-phase attack.

Risk and Mitigation:

Just as recipients of strange email attachments should be cautious about opening them, programs that process DICOM media files should take precautions. Virus scanning software should scan DICOM media files and not assume DICOM media files are safe. DICOM files are never intended to hold executable code, so DICOM media files should never be given executable file extensions, and finding an executable code inside a DICOM media file should trigger warning flags. Data import systems should have file execution disabled when reading CD/DVDs.

The CDs and DVDs themselves are read-only, and not easy to counterfeit. Media files on a USB stick, email attachments, or shared over the web are only as safe as the associated security systems. For example, the Dental profile for email exchange requires the use of encryption for DICOM files.

DICOM images read from media and sent over the network using DICOM protocols (C-Store, C-Move, C-Get) have the preamble stripped off before sending, so they would not pass an infected preamble into a downstream system, like a PACS or VNA. DICOM images read from media and sent using DICOM Web services (e.g., STOW-RS, WADO-RS), however, may pass the preamble, so care must be taken by the application to ensure that if a preamble exists, it is a known preamble such as TIFF. If not, the preamble should be cleared (set to 00H).

DICOM receivers commonly add a blank preamble (128 bytes of 00H) onto images they receive. All of the DICOM images in your VNA or PACS should either not contain the preamble, or contain a known safe preamble.

The PACS or VNA needs strong access control, logging, and audit monitoring to ensure that DICOM files are not maliciously altered by unauthorized agents. A file validity scanner can help detect unauthorized modifications.

FAQs

1.) Are the DICOM files in my archive (PACS or VNA) at risk and if so what can I do to protect them?

The preamble issue does not change the risks to an archive. The media importers generally strip or validate headers on input, removing any malicious preamble before sending the data to the archive. The other risks from unauthorized access or modification remain the same as before. Archives must be protected in general from hostile access.

2.) How can I determine if any of the DICOM files in my archive (PACS or VNA) have been maliciously altered?

There is no concern from the preamble vulnerability if the archive stores the files in a database structure or non-DICOM file format.

If the archive stores files in Part10 format, the preamble should be verified to be either cleared or one of the known safe headers. For example, a TIFF preamble starts with four bytes containing either “MM\x00\x2a” or “II\x2a\x00”. Anything else should trigger a local warning if an executable preamble is found issue a security warning and clear the preamble.

A more extensive step of clearing the preamble will not interfere with DICOM uses but would remove another compatibility (e.g., TIFF) that may be wanted.

3.) We receive DICOM studies brought by patients on CD/DVDs. What should we do to be sure they do not contain malware or infect our systems?

CD/DVDs originally created by the imaging center should be safe. However, it is a good practice always to verify that the preamble is a known format or clear the preamble. Never execute any DICOM file on CD/DVD.

4.) Could opening, viewing, or copying the images on the CD/DVD infect the computer being used?

No. The DICOM viewers and an ordinary file copy do not execute the file. Do not ever attempt to execute a DICOM file. It is always a good idea to enable malware detection.

5.) Can you recommend malware scanning software that we can use on our CD/DVDs that would detect infected DICOM files?

As a Standards Development Organization, we do not make specific product recommendations.

6.) We receive DICOM studies sent electronically from different medical centers and uploaded by patients using web software. How can we prevent these studies from introducing malware into our hospital?

The preamble should be verified to be either cleared or one of the known safe headers. For example, a TIFF preamble starts with four bytes containing either “MM\x00\x2a” or “II\x2a\x00”. Anything else should trigger a local warning. If an executable preamble is found issue a security warning and clear the preamble, the security warning should also be sent back to the source so that they can track down their security issue.

A more extensive step of clearing the preamble will not interfere with DICOM uses but would remove another compatibility (e.g., TIFF) that may be wanted.

7.) We are planning to switch our traditional DICOM C-Store and C-Move services over to DICOM Web. What should we do to detect malicious preambles and block them from being sent or retrieved?

Check with vendors that they verify or clear preambles before sending and receiving images. Most already do. If you are writing your software, see the answer to 6.) above.

8.) Who uses this preamble feature today?

It is being used in digital microscopy, where there is a large base of software that expects the TIFF format.

It is being used in medical research; for example, it is a planned feature of The Cancer Imaging Archive (TCIA – https://www.cancerimagingarchive.net).

9.) If the software we use to read outside CD/DVDs can zero or ignore the preamble, does that break anything?

It has no impact on DICOM operations. DICOM systems ignore the preamble. Clearing the preamble will remove TIFF or similar compatibility if it was previously there. That might interfere with microscopy, research, and similar uses.

10.) Should patients be concerned about the CD/DVDs that they are given after imaging studies?

No. The CD/DVDs created at the imaging facility are created with clean or known safe preambles. The CD/DVDs should be safely stored for later use. Copies kept on a local computer could be modified if the computer security is breached.

For further information, please contact Lisa Spellman, DICOM General Secretary, dicom@dicomstandard.org