DICOM Correction Proposal

STATUS	Final Text
Date of Last Update	2020/01/17
Person Assigned	Rob Horn
Submitter Name	Rob Horn rjhorniii@gmail.com
Submission Date	2019/05/28

Correction Number CP- 1948
Log Summary: Part 10 Format security considerations
Name of Standard PS3.10, PS3.18 2019e
Rationale for Correction: This is a response to a vulnerability report assigned CVE-2019-11687. When the CP is approved, the CVE maintainers should be formally notified that the DICOM Standard has been updated.
Correction Wording:

Add 7.5 Security Considerations to PS3.10 (Media)

7.5 SECURITY CONSIDERATIONS FOR DICOM FILE FORMAT

The DICOM File Format has a potential security vulnerability when the 128-byte File Preamble contains malicious executable content. Such malicious executable content may also refer to other malicious content in the file hidden within Data Elements of the File Meta Information or the Data Set.

Depending upon the use and purpose of a particular application it may be appropriate to:

- Sanitize the preamble, such as by:
  - Verifying that the preamble is:
    - all zeroes, or
    - begins with a valid magic number for recognized dual format content (e.g., TIFF or BigTIFF), or
    - contains other known safe content.
  - Clearing the preamble regardless of its content

    Note. This will prevent use by applications that depend on the non-DICOM format, if the dual format capability has been used.

  - Testing explicitly for executable preamble contents.

    Note. The proper response to the presence of executable content depends upon the purpose of the application, but generally, legitimate executable content will not be found in a DICOM File. A hypothetical example of an exception would be if the file contained its own executable viewer; this is sufficiently unlikely as to be not worth considering.

- Test explicitly for executable content anywhere within the DICOM File.
- Validate that the DICOM values, structures and content comply with the standard encoding rules and the IOD of the specified SOP Class, including Private Data Elements.

Note. Validation that Data Element Values comply with their Value Representation may partially mitigate the risk of hidden malicious content, but it may be necessary to remove or analyze the contents of opaque binary data in OB or other binary numeric value Data Elements, whether they be Standard or Private Data Elements. The VR of Private Data Elements may not be known. Without an executable preamble, such hidden content may not be directly executable, but may still serve as a repository of malicious code to be activated by some other accompanying exploit.

- Validate that the contents are of the appropriate SOP Classes.
- Validate that DICOM File Format files created for HTTP requests and responses do not contain such malicious content.

  Note: For example, it may be appropriate for an archive that stores and retrieves PS3.10 Files to verify and validate both input and output, rather than store and retrieve files without checking the content.

The proper response to a validation failure depends upon the purpose of the application. Validation might be performed on input, output, or both.

Note: For example, an archive may choose to sanitize SOP Instances upon receipt, sanitize SOP Instances upon retrieval, validate the structure and fail storage requests for SOP Instances that fail validation, or other behavior based on the product purpose and the threat environment. This behavior is not specified by DICOM because the product purpose and the threat environment are highly dependent upon the application.

An implementation shall describe in its Conformance Statement its behavior with respect to sanitization of the preamble and any other validation performed.

Amend in PS3.10 Section 9 Conformance:

An implementation of PS3.10 shall:

a. have a Conformance Statement based on a PS3.11 Application Profile in accordance with the framework defined in PS3.2**, which will include addressing the Security Requirements defined in Section 7.5**;

b. meet the requirements of the DICOM File Format as specified in Section 7;

c. support the DICOM File Service as specified in Section 8, in one or more of the roles identified in Section 8.3;

d. perform the Media Operations defined in Table 8.3-1 according to the role supported;

e. support the DICOMDIR File with a content as specified in the Media Storage Directory SOP Class in PS3.4.

Amend in PS3.18 Section 6 Conformance:

An implementation claiming conformance to this Part of the Standard shall function in accordance with all its mandatory sections.

DICOM Web Services are used to transmit Composite SOP Instances. All Composite SOP Instances transmitted shall conform to the requirements specified in other Parts of the Standard.

An implementation may conform to the DICOM Web Services by supporting the role of origin server or user agent, or both, for any of the Services defined in this Part of the Standard. The structure of Conformance Statements is specified in PS3.2.

An implementation shall describe in its Conformance Statement the Real-World Activity associated with its use of DICOM Web Services, including any proxy functionality between a Web Service and the equivalent DIMSE Service.

An implementation shall describe in its Conformance Statement the security mechanisms utilized by the implementation. **See Section 8.11.**

Modify 8.11 Security and Privacy in PS3.18 Web Services:

8.11 SECURITY AND PRIVACY

It is very likely that DICOM objects contain Protected Health Information. Privacy regulations in the United States (HIPAA), Europe (GDPR), and elsewhere, require that Individually Identifiable Information be kept private. It is the responsibility of ~~**implementers of**~~ **those implementing and deploying** the DICOM Standard to ensure that ~~**governmental**~~ **applicable** regulations for security and privacy are satisfied.

See, for example, [ONC Privacy Security Guide].

The DICOM PS3.10 File Format has security considerations that will apply whenever DICOM PS3.10 File format is used. See PS3.10 Section 7.5.