

DCMTK - Bug #970

Incorrect handling of malformed JPEG bitstream

2021-03-04 10:32 - Marco Eichelberg

Status:	Closed	Start date:	2021-03-04
Priority:	Normal	Due date:	
Assignee:	Marco Eichelberg	% Done:	0%
Category:	Library	Estimated time:	2:00 hours
Target version:	3.6.7	Compiler:	
Module:	dcmjpeg		
Operating System:			
Description			
Apparently the IJG JPEG code embedded into DCMTK does not correctly handle certain invalid JPEG bitstreams that contain inconsistent start-of-scan (SOS) markers. The issue is discussed in https://bugs.chromium.org/p/chromium/issues/detail?id=258723 and has been fixed in Chromium and libjpeg-turbo. The fix can be readily applied to DCMTK as well:			
<pre>diff --git a/dcmjpeg/libijg12/jdmarker.c b/dcmjpeg/libijg12/jdmarker.c index 355835c7f..4d1e63f84 100644 --- a/dcmjpeg/libijg12/jdmarker.c +++ b/dcmjpeg/libijg12/jdmarker.c @@ -346,6 +346,12 @@ @@ get_sos (j_decompress_ptr cinfo) compptr->dc_tbl_no, compptr->ac_tbl_no); } + /* This CSi (cc) should differ from the previous CSi */ + for (ci = 0; ci < i; ci++) { + if (cinfo->cur_comp_info[ci] == compptr) + ERREXIT1(cinfo, JERR_BAD_COMPONENT_ID, cc); + } + /* Collect the additional scan parameters Ss, Se, Ah/Al. */ INPUT_BYTE(cinfo, c, return FALSE); cinfo->Ss = c; diff --git a/dcmjpeg/libijg16/jdmarker.c b/dcmjpeg/libijg16/jdmarker.c index f2b6188e8..381f58226 100644 --- a/dcmjpeg/libijg16/jdmarker.c +++ b/dcmjpeg/libijg16/jdmarker.c @@ -346,6 +346,12 @@ @@ get_sos (j_decompress_ptr cinfo) compptr->dc_tbl_no, compptr->ac_tbl_no); } + /* This CSi (cc) should differ from the previous CSi */ + for (ci = 0; ci < i; ci++) { + if (cinfo->cur_comp_info[ci] == compptr) + ERREXIT1(cinfo, JERR_BAD_COMPONENT_ID, cc); + } + /* Collect the additional scan parameters Ss, Se, Ah/Al. */ INPUT_BYTE(cinfo, c, return FALSE); cinfo->Ss = c; diff --git a/dcmjpeg/libijg8/jdmarker.c b/dcmjpeg/libijg8/jdmarker.c index 22f18e567..d7d4a1c37 100644 --- a/dcmjpeg/libijg8/jdmarker.c +++ b/dcmjpeg/libijg8/jdmarker.c @@ -346,6 +346,12 @@ @@ get_sos (j_decompress_ptr cinfo) compptr->dc_tbl_no, compptr->ac_tbl_no); } + /* This CSi (cc) should differ from the previous CSi */</pre>			

```
+ for (ci = 0; ci < i; ci++) {
+   if (cinfo->cur_comp_info[ci] == compptr)
+     ERREXIT1(cinfo, JERR_BAD_COMPONENT_ID, cc);
+ }
+
+ /* Collect the additional scan parameters Ss, Se, Ah/Al. */
+ INPUT_BYTE(cinfo, c, return FALSE);
+ cinfo->Ss = c;
```

Reported 2021-03-04 by Christian Wetzel <wetzel@phoenix-pacs.de>.

History

#1 - 2021-03-04 10:32 - Marco Eichelberg

- Category set to Library
- Target version set to 3.6.7
- Module set to dcmjpeg

#2 - 2021-03-04 11:06 - Marco Eichelberg

- File issue_970.dcm added

The attached JPEG-compressed DICOM image, based on https://lcamtuf.coredump.cx/jpeg_leak/, demonstrates the issue. The output of a "jpegdump" of the JPEG bitstream contains the following section:

```
Offset 0x0130 Marker 0xffda SOS Start of Scan length variable 0x0c
  JPEG_SOS_Parameters:
    nComponentsPerScan = 3
    component 0
      ScanComponentSelector = 3
      DCEntropyCodingTableSelector = 0
      ACEntropyCodingTableSelector = 0
      MappingTableSelector(LS) = 0
    component 1
      ScanComponentSelector = 2
      DCEntropyCodingTableSelector = 1
      ACEntropyCodingTableSelector = 1
      MappingTableSelector(LS) = 17
    component 2
      ScanComponentSelector = 3
      DCEntropyCodingTableSelector = 1
      ACEntropyCodingTableSelector = 1
      MappingTableSelector(LS) = 17
    StartOfSpectralOrPredictorSelection/NearLosslessDifferenceBound(LS) = 0
    EndOfSpectralSelection/InterleaveMode(LS) = 63
    SuccessiveApproximationBitPositionHigh = 0
    SuccessiveApproximationBitPositionLowOrPointTransform = 0
```

Note that component 0 and 2 both have "ScanComponentSelector = 3", and there is no entry with "ScanComponentSelector = 1". dcmdjpeg should refuse to decode this image, because doing so would cause uninitialized memory to appear in the output, but currently only prints a warning and produces a decompressed image.

#3 - 2021-03-05 13:28 - Marco Eichelberg

- Status changed from New to Closed
- Assignee set to Marco Eichelberg
- Estimated time set to 2:00 h

Closed by commit #e8161b1e4.

Files

issue_970.dcm	1.46 KB	2021-03-04	Marco Eichelberg
---------------	---------	------------	------------------