# DCMTK - Bug #1134

## Vulnerabilities in the JPEG library

2024-08-23 15:41 - Marco Eichelberg

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 2024-08-23 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | | **% Done:** | 100% |
| **Category:** | Library and Apps | **Estimated time:** | 0:00 hour |
| **Target version:** | 3.7.1+ | | |
| **Module:** | dcmjpeg | **Compiler:** | |
| **Operating System:** | | | |

**Description**

The JPEG library in the dcmjpeg module, which is derived from the IJG libjpeg 6b, contains the following vulnerabilities, which have been reported for other libraries derived from the same code:

NVD - CVE-2020-14153
https://nvd.nist.gov/vuln/detail/CVE-2020-14153

NVD - CVE-2020-14152
https://nvd.nist.gov/vuln/detail/CVE-2020-14152

Reported 2024-08-22 by Bert Knops <bert.knops@pie.nl>.

### History

#### #1 - 2024-12-24 20:12 - Marco Eichelberg

*- % Done changed from 0 to 50*

The bug fix implemented in libjpeg 9d for CVE-2020-14153 is the following code fragment:

```
-     entropy->ac_cur_tbls[blkn] = entropy->ac_derived_tbls[compptr->ac_tbl_no];
+     entropy->ac_cur_tbls[blkn] =    /* AC needs no table when not present */
+    cinfo->lim_Se ? entropy->ac_derived_tbls[compptr->ac_tbl_no] : NULL;
```

The bug is analyzed in detail here: https://github.com/libjpeg-turbo/libjpeg-turbo/issues/445

Without a sample image that demonstrates the issue it is difficult to determine this for certain,
but since this code does not exist at all in the version of libjpeg used in DCMTK, and since
there is no lim_Se in our version of the jpeg_decompress_struct, it seems that this bug does not affect DCMTK, in any version.

#### #2 - 2024-12-24 20:20 - Marco Eichelberg

*- Status changed from New to Closed*

*- % Done changed from 50 to 100*

CVE-2020-14152 is related to the max_memory_to_use member of struct jpeg_memory_mgr. This is the fix:

```
GLOBAL(long)
jpeg_mem_available (j_common_ptr cinfo, long min_bytes_needed,
                    long max_bytes_needed, long already_allocated)
{
+  if (cinfo->mem->max_memory_to_use)
+    return cinfo->mem->max_memory_to_use - already_allocated;
+
+  /* Here we say, "we got all you want bud!" */
  return max_bytes_needed;
}
```

The version of libjpeg used in DCMTK does not support max_memory_to_use. That means that DCMTK is not affected by CVE-2020-14152, although the problem that images may consume a lot of memory during decompression of course also exists.