DCMTK - Bug #1108

Possible overflow in EctEnhancedCT

2024-02-21 11:17 - Michael Onken

Status:	Closed	**Start date:**	2024-02-21
Priority:	Normal	**Due date:**	
Assignee:	Michael Onken	**% Done:**	100%
Category:	Library	**Estimated time:**	1:00 hour
Target version:			
Module:	dcmect	**Compiler:**	
Operating System:			

Description

The first problem stems from the fact that the multiplication of rows and cols may overflow 'int' before it is converted to 'size_t'. For example, if the EctEnhancedCT::create method is used where a user has control over the value of rows and cols.

```
Uint16 rows = 0;
Uint16 cols = 0;
m_CT.getRows(rows);
m_CT.getColumns(cols);
const size_t numFrames      = m_CT.m_Frames.size();
const size_t numBytesFrame  = m_CT.m_Frames[0]->length;
// HERE:
const size_t numPixelsFrame = rows * cols;
```

Inside the below method the expected number of pixel bytes is not validated, leading to uncontrolled access to memory in a memcpy() call.

```
OFCondition EctEnhancedCT::WriteVisitor::operator()(ImagePixel& pixel)
```

This has been fixed in commit #ec52e9.

Thanks to GitHub user "bananabr" (Daniel Berredo) for the report and suggested patch.