DCMTK - Bug #1120

Segmentation faults due to incorrect typecast of DcmItem::search() result

2024-04-12 14:50 - Marco Eichelberg

Status:	Closed	**Start date:**	2024-04-12
Priority:	High	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library and Apps	**Estimated time:**	6:00 hours
Target version:	3.6.9		
Module:		**Compiler:**	
Operating System:			

Description

DcmItem::search() returns the search result in the form of a stack of pointers to DcmObject instances.
In most cases, the code that performs a search performs a typecast after a successful search.
Apparently, in some places the code does not check the type of the search result before performing the typecast.
This can lead to a segmentation fault if a DICOM object containing elements with incorrect VR is processed.
For example, the attached sample file will cause a segmentation fault when the following command is executed:

```
dcmpsmk sample.dcm output.dcm
```

The reason for the segfault is this element in the dataset:

```
(0028,3010) CS [00]                                     #   2, 1 VOILUTSequence
```

Code in module dcmpstat will cast the DcmObject * returned by DcmItem::search(), which in fact points to an instance of DcmCodeString, to DcmSequenceOfItems and then call a method of class DcmSequenceOfItems, causing the segfault.
All instances in the toolkit where the result of DcmItem::search() is typecasted must perform a check of the class to be casted to, e.g. using DcmObject::ident(). This should be checked in all cases.

Reported 2024-04-08 by Cisco Talos as Security Advisory TALOS-2024-1957.

History

#1 - 2024-04-22 11:45 - Marco Eichelberg

- Status changed from New to Closed

- Assignee set to Marco Eichelberg

- % Done changed from 0 to 100

- Estimated time set to 6:00 h

Fixed by commit #601b227ee for DCMTK public and #51081a8cc for the private modules.

#2 - 2024-04-24 09:52 - Marco Eichelberg

- Private changed from Yes to No

The security advisory from Cisco Talos as now publicly available at https://talosintelligence.com/vulnerability_reports/TALOS-2024-1957

Files

sample.dcm	16.9 KB	2024-04-12	Marco Eichelberg