DCMTK - Bug #1167

Issue rendering invalid monochrome image

2025-11-06 17:21 - Marco Eichelberg

Status:	Closed	**Start date:**	2025-11-06
Priority:	Normal	**Due date:**	
Assignee:	Jörg Riesmeier	**% Done:**	100%
Category:		**Estimated time:**	0:00 hour
Target version:			
Module:		**Compiler:**	
Operating System:			

Description

There is an issue in class DicomImage when rendering an invalid monochrome DICOM image where the number of pixels stored does not match the expected number of pixels. If the stored number is less than the expected number, the rest of the pixel matrix for the intermediate representation was always filled with the value 0. Under certain, very rare conditions, this could result in memory problems reported by an Address Sanitizer (ASAN). Now, the rest of the matrix is filled with the smallest possible value for the image.

Thanks to Emmanuel Tacheau from the Cisco Talos team <vulndiscovery@external.cisco.com> for the original report, the sample file (PoC) and further details.

Fixed in commit #89a6e399f.

This issue has been registered as TALOS-2024-2122 and CVE-2024-47796. (https://www.cve.org/CVERecord?id=CVE-2024-47796).