DCMTK - Bug #1175

Possible overflows and underflows in ACSE data structures

2025-11-06 18:01 - Marco Eichelberg

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

Description

At several places in the code a wrong length of ACSE data structures received over the network can cause overflows or underflows when processing those data structures. Related checks have been added at various places in order to prevent such (possible) attacks.

Thanks to Kevin Basista for the report.

Closed by commit #1b6bb7607.

This issue has been registered as CVE-2015-8979 (https://www.cve.org/CVERecord?id=CVE-2015-8979).