DCMTK - Bug #1196

SEGV via OOB Read in DcmJSONReader getTokenContent

2026-03-25 10:09 - Jörg Riesmeier

Status:	Closed	**Start date:**	2026-03-25
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library	**Estimated time:**	0:00 hour
Target version:	3.7.1		
Module:	dcmdata	**Compiler:**	
Operating System:			

Description

Received by email from the IN-CYPHER OSS Security Team (2026-03-24):

> **Subject:** IC-DCMTK-0008 SEGV via OOB Read in DcmJSONReader getTokenContent
> **Version:** DCMTK master 418274445 (DCMTK-3.7.0+64)
> **CWE:** CWE-125 (Out-of-bounds Read)
>
> This report describes a SEGV crash in `DcmJSONReader::getTokenContent()`, sharing the same JSMN two-pass token mismatch root cause as IC-DCMTK-0006 but manifesting differently. In this variant, the corrupted token offsets compute to addresses that fall in unmapped virtual memory pages, causing a hard SIGSEGV regardless of sanitizer instrumentation.
>
> Note: Like IC-DCMTK-0007, our current PoC requires the `--ignore-errors` flag to reproduce. We have not yet constructed a PoC that bypasses this requirement, but we report this issue out of caution because the underlying `getTokenContent()` function lacks bounds validation regardless of the error policy setting. We report this separately from IC-DCMTK-0006 because without ASan, IC-DCMTK-0006's heap OOB may silently succeed, while this variant always crashes. A 25-byte malformed JSON input triggers immediate process termination.
>
> Please find the detailed report, proof-of-concept, and sanitizer output in the attachments.

Related issues:

Related to DCMTK - Bug #1193: Heap OOB Read in DcmJSONReader getTokenContent	**Closed**	**2026-03-10**
Related to DCMTK - Bug #1195: Heap OOB Read via PersonName Path in DcmJSONReader	**Closed**	**2026-03-25**

History

#1 - 2026-03-29 09:02 - Marco Eichelberg

- Related to Bug #1193: Heap OOB Read in DcmJSONReader getTokenContent added

#2 - 2026-03-29 09:03 - Marco Eichelberg

- Related to Bug #1195: Heap OOB Read via PersonName Path in DcmJSONReader added

#3 - 2026-03-29 09:03 - Marco Eichelberg

- Status changed from New to Closed

- Assignee set to Marco Eichelberg

- % Done changed from 0 to 100

- Estimated time set to 0:00 h

Closed by commit #4add0621b (i.e. the same commit that also closed DCMTK issue #1193.)

#4 - 2026-03-30 18:49 - Marco Eichelberg

- Private changed from Yes to No

Files

IC-DCMTK-0008_crash_output.txt	1.76 KB	2026-03-25	Jörg Riesmeier
IC-DCMTK-0008_poc.json	142 Bytes	2026-03-25	Jörg Riesmeier
IC-DCMTK-0008_REPORT.md	3.69 KB	2026-03-25	Jörg Riesmeier