DCMTK - Bug #1195

Heap OOB Read via PersonName Path in DcmJSONReader

2026-03-25 10:06 - Jörg Riesmeier

Status:	Closed	**Start date:**	2026-03-25
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library	**Estimated time:**	1:00 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-0007 Heap OOB Read via PersonName Path in DcmJSONReader
> **Version:** DCMTK master 418274445 (DCMTK-3.7.0+64)
> **CWE:** CWE-125 (Out-of-bounds Read)
>
> This report describes a heap buffer overflow in
> getTokenContent() reached through the PersonName (PN VR) processing path
> in parseElementValueArray() at dcjsonrd.cc:1022. While this shares the same
> JSMN two-pass root cause as IC-DCMTK-0006, it is reached through a third,
> independent call site that a fix addressing only the parseElement() call
> sites would miss. This variant requires the --ignore-errors flag (setting
> stopOnErrorPolicy_ to OFFalse), which is why we rate it as high rather than
> critical. A 44-byte JSON input triggers the out-of-bounds read.
>
> Please find the detailed report, proof-of-concept, and sanitizer output
> in the attachments.

Follow-up message:

> This bug shares the JSMN two-pass root cause with IC-DCMTK-0006 but is
> reached through a third independent call site that a targeted fix would
> miss. Our PoC currently requires --ignore-errors; we report it preemptively
> since the code path lacks bounds validation regardless of error policy.

Related issues:

Related to DCMTK - Bug #1193: Heap OOB Read in DcmJSONReader getTokenContent	**Closed**	**2026-03-10**
Related to DCMTK - Bug #1196: SEGV via OOB Read in DcmJSONReader getTokenContent	**Closed**	**2026-03-25**

History

#1 - 2026-03-25 10:09 - Jörg Riesmeier

- Description updated

#2 - 2026-03-28 20:08 - Marco Eichelberg

- Status changed from New to Closed

- Assignee set to Marco Eichelberg

- % Done changed from 0 to 100

- Estimated time set to 1:00 h

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

#3 - 2026-03-28 20:09 - Marco Eichelberg

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

#4 - 2026-03-29 09:03 - Marco Eichelberg

- Related to Bug #1196: SEGV via OOB Read in DcmJSONReader getTokenContent added

#5 - 2026-03-30 18:49 - Marco Eichelberg

- Private changed from Yes to No

Files

IC-DCMTK-0007_crash_output.txt	3.3 KB	2026-03-25	Jörg Riesmeier
IC-DCMTK-0007_poc.json	44 Bytes	2026-03-25	Jörg Riesmeier
IC-DCMTK-0007_REPORT.md	3.9 KB	2026-03-25	Jörg Riesmeier