DCMTK - Bug #1197

Uninitialized Memory Read in JSMN Token Array

2026-03-25 10:11 - 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-0009 Uninitialized Memory Read in JSMN Token Array
> **Version:** DCMTK master 418274445 (DCMTK-3.7.0+64)
> **CWE:** CWE-908 (Use of Uninitialized Resource)
>
> This report describes a uninitialized memory read in the JSON DICOM reader.
> The reserveTokens() function allocates tokenNum+1 JSMN tokens but the memset
> at dcjsonrd.cc:200 only initializes the first tokenNum elements. While the
> sentinel token's start, end, and size fields are explicitly set, the type
> field is left containing heap garbage. When malformed JSON causes the token
> pointer to advance into the sentinel position, the uninitialized type field
> is read in a switch statement, causing undefined behavior. UBSan confirms
> the issue, reporting invalid enum values. A 40-byte PoC triggers this bug.
>
> Please find the detailed report, proof-of-concept, and sanitizer output
> in the attachments.

History

#1 - 2026-03-25 10:15 - Jörg Riesmeier

- Description updated

#2 - 2026-03-29 10:05 - 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 #ae94a3d75.

#3 - 2026-03-30 18:50 - Marco Eichelberg

- Private changed from Yes to No

Files

IC-DCMTK-0009_crash_output.txt	1.39 KB	2026-03-25	Jörg Riesmeier
IC-DCMTK-0009_poc.json	40 Bytes	2026-03-25	Jörg Riesmeier
IC-DCMTK-0009_REPORT.md	2.61 KB	2026-03-25	Jörg Riesmeier