# DCMTK - Bug #1193

## Heap OOB Read in DcmJSONReader getTokenContent

2026-03-10 23:46 - Jörg Riesmeier

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 2026-03-10 |
| **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 (2026-03-09):

> **Subject:** IC-DCMTK-0006 Heap OOB Read in DcmJSONReader getTokenContent
> **Version:** DCMTK master 418274445 (DCMTK-3.7.0+64)
> **CWE:** CWE-122 (Heap-based Buffer Overflow)
>
> This report details a heap buffer overflow in `DcmJSONReader::getTokenContent()` at `dcjsonrd.cc:221`.
> The JSMN tokenizer's two-pass parsing mechanism can produce a sentinel token (with `start=INT_MAX, end=INT_MAX`) when the code reads past the allocated token array. The `getTokenContent()` function uses these unvalidated position fields to index into the JSON input buffer, causing out-of-bounds heap reads and writes. A malformed JSON input as small as 8 bytes triggers this vulnerability without requiring any special flags — the default `json2dcm` invocation crashes immediately.
>
> Please find the detailed report, proof-of-concept, and sanitizer output in the attachments.

**Related issues:**

| | | |
|---|---|---|
| Related to DCMTK - Bug #1195: Heap OOB Read via PersonName Path in DcmJSONReader | **Closed** | **2026-03-25** |
| Related to DCMTK - Bug #1196: SEGV via OOB Read in DcmJSONReader getTokenContent | **Closed** | **2026-03-25** |

## History

**#1 - 2026-03-10 23:54 - Jörg Riesmeier**

*- Description updated*

**#2 - 2026-03-10 23:56 - Jörg Riesmeier**

*- Description updated*

**#3 - 2026-03-28 18:22 - Marco Eichelberg**

*- Assignee changed from Tingyan Xu to Marco Eichelberg*

*- % Done changed from 0 to 100*

*- Estimated time set to 1:00 h*

*- Status changed from New to Closed*

Closed by commit #4add0621b.

**#4 - 2026-03-28 20:09 - Marco Eichelberg**

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

**#5 - 2026-03-29 09:02 - Marco Eichelberg**

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

**#6 - 2026-03-30 18:49 - Marco Eichelberg**

*- Private changed from Yes to No*

### Files

| | | | |
|---|---|---|---|
| IC-DCMTK-0006_crash_output.txt | 1.65 KB | 2026-03-10 | Jörg Riesmeier |
| IC-DCMTK-0006_poc.json | 19 Bytes | 2026-03-10 | Jörg Riesmeier |
| IC-DCMTK-0006_REPORT.md | 3.65 KB | 2026-03-10 | Jörg Riesmeier |