DCMTK - Bug #1189

Double-Free in DcmJSONReader via decodeBase64()

2026-03-09 16:55 - Jörg Riesmeier

Status:	Closed	**Start date:**	2026-03-09
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Library	**Estimated time:**	2:00 hours
Target version:	3.7.1		
Module:	ofstd, dcmdata	**Compiler:**	
Operating System:			

Description

Received by email from the IN-CYPHER OSS Security Team (2026-03-09):

> **Subject:** IC-DCMTK-0002: Double-Free in DcmJSONReader via decodeBase64()
> **Version:** DCMTK master 418274445 (DCMTK-3.7.0+64)
> **CWE:** CWE-415 (Double Free)
>
> This report details a double-free vulnerability in
> the JSON DICOM reader's inlineBinary processing path. When
> OFStandard::decodeBase64() receives invalid base64 input containing
> fewer than 4 valid characters, it internally frees the allocated output
> buffer at ofstd.cc:1892 but does not nullify the pointer. The calling
> code in parseElement() at dcjsonrd.cc:752 then unconditionally executes
> delete[] data, freeing the same memory a second time. A 43-byte JSON
> input with a single-character base64 value triggers this heap
> corruption.
>
> Please find the detailed report, proof-of-concept, and sanitizer output
> in the attachments.

History

#1 - 2026-03-09 16:56 - Jörg Riesmeier

- Status changed from New to Closed

- % Done changed from 0 to 100

- Estimated time set to 1:00 h

Closed by commit 28e3a0031.

#2 - 2026-03-10 10:41 - Jörg Riesmeier

- Estimated time changed from 1:00 h to 2:00 h

- Private changed from Yes to No

#3 - 2026-03-10 23:53 - Jörg Riesmeier

- Description updated

#4 - 2026-03-10 23:59 - Jörg Riesmeier

- Description updated

Files

IC-DCMTK-0002_poc.json	43 Bytes	2026-03-09	Jörg Riesmeier
IC-DCMTK-0002_crash_output.txt	2.77 KB	2026-03-09	Jörg Riesmeier
IC-DCMTK-0002_REPORT.md	3.54 KB	2026-03-09	Jörg Riesmeier