DCMTK - Bug #1198

Path Traversal in JSON Bulkdata Loading

2026-03-25 10:14 - 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-0024: Path Traversal in JSON Bulkdata Loading
> **Version:** DCMTK master 418274445 (DCMTK-3.7.0+64)
> **CWE:** CWE-22 (Path Traversal)
>
> This report describes a TOCTOU (time-of-check-to-time-of-use) race condition in DcmJSONReader::loadBulkdataFile() at dcjsonrd.cc:694-710. While the code correctly implements path canonicalization via realpath() and checks against permitted directories, a race window exists between the realpath() resolution and the subsequent fopen() call. An attacker with write access to a permitted directory could theoretically swap a symlink in this window to redirect the file read outside the permitted directory. We rate this as limited practical exploitability because practical exploitation requires multiple prerequisites: local filesystem write access to a permitted directory, precise timing to win the microsecond-scale race window, and an application configured with permitted bulkdata directories.
>
> Please find the detailed report and suggested fix in the attachments.

History

#1 - 2026-03-29 14:51 - 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 #969c4b6f2.

#2 - 2026-03-30 18:50 - Marco Eichelberg

- Private changed from Yes to No

Files

IC-DCMTK-0024_poc_bulkdata.json	554 Bytes	2026-03-25	Jörg Riesmeier
IC-DCMTK-0024_REPORT.md	2.56 KB	2026-03-25	Jörg Riesmeier
IC-DCMTK-0024_toctou_poc.cc	4.34 KB	2026-03-25	Jörg Riesmeier