# DCMTK - Bug #1199

## Security Vulnerability Report: Remote Heap Buffer Overflow in dcmqrscp (deleteOldestImages)

2026-04-02 14:35 - Jörg Riesmeier

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 2026-04-02 |
| **Priority:** | High | **Due date:** | |
| **Assignee:** | | **% Done:** | 100% |
| **Category:** | Library | **Estimated time:** | 0:00 hour |
| **Target version:** | 3.7.1 | | |
| **Module:** | dcmqrdb | **Compiler:** | |
| **Operating System:** | | | |

**Description**

Report by email from "elp3pinill0" (2026-03-29):

=== CUT ===

I am writing to report a critical security vulnerability I have identified in DCMTK (v3.7.0+ DEV).

The vulnerability is a Remote Heap Buffer Overflow located in the dcmqrscp application, specifically within the database management logic. This flaw could allow a remote attacker to corrupt heap memory, potentially leading to a Denial of Service (DoS) or Remote Code Execution (RCE) on the server.

## Vulnerability Details

- Component: dcmqrdb / dcmqrscp
- File: dcmqrdb/libsrc/dcmqrdbi.cc
- Function: DcmQueryRetrieveIndexDatabaseHandle::deleteOldestImages()
- Type: Heap-based Buffer Overflow (Out-of-Bounds Write)
- Impact: High/Critical (Remote exploitation possible via DICOM C-STORE)

## Root Cause Analysis

In dcmqrdbi.cc, a heap array StudyArray is allocated with a fixed size of MAX_NUMBER_OF_IMAGES (defined as 10,000 in dcmqridx.h).

*[image removed]*

The code then enters an unbounded loop to populate this array by iterating through the index database. There is no bounds check on the nbimages counter before writing to the array. If a study contains more than 10,000 images and the storage quota (maxBytesPerStudy) is exceeded, the function writes past the end of the StudyArray buffer.

*[image removed]*

## Proof of Concept (PoC) & Reproduction

I have successfully reproduced this crash using the following environment:

- OS: Kali Linux (x86_64)
- DCMTK Version: v3.7.0+ DEV (Build: cxx11 threads lfs)

- Steps:

1. Configure dcmqrscp with a MaxBytesPerStudy quota (e.g., 7MB).

*[image removed]*

2. Run it with the following command: sudo dcmqrscp -c dcmqrscp.cfg -v 104 --acse-timeout 300 --dimse-timeout 300

3. Send >12,000 DICOM instances sharing the same StudyInstanceUID using storescu.

*[image removed]*

4. You can use the following commands and template provided to generate dcm:

*[image removed]*

5. Send C-STORE request with image_x.dcm: dcmsend -v --max-pdu 131072 --no-halt --aetitle TESTCLIENT --call TESTSTORE localhost 104 image_*.dcm

*[image removed]*

6. Once the quota is reached, checkupinStudyDesc() triggers deleteOldestImages(), causing the Heap overflow.

.

## Severity Assessment (CVSS v4.0)

- Vector: CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N
- Base Score: 9.2 (Critical)
  - Attack Requirements (AT:P): The vulnerability requires a specific configuration where the MaxBytesPerStudy quota is enabled and active.
  - Exploitability: While a Heap Overflow is inherently complex to weaponize, the lack of an immediate segmentation fault (DoS) suggests a silent heap metadata corruption. This provides an attacker with a primitive for "heap grooming," significantly increasing the feasibility of achieving Remote Code Execution (RCE).
  - Impact: A successful exploit would compromise the integrity and confidentiality of the medical imaging database. Availability is marked as "Low" because the system may remain operational in an unstable state after the malloc corruption occurs.

## Proposed Fix

A boundary check should be implemented in the loop within deleteOldestImages to ensure nbimages never exceeds MAX_NUMBER_OF_IMAGES, or alternatively, the array should be replaced with a dynamic container like std::vector.

I am following responsible disclosure practices and would appreciate a confirmation of receipt. Please let me know if you require further details or specific files to verify the fix.

**Related issues:**

| | | |
|---|---|---|
| Has duplicate DCMTK - Bug #1206: Remote Heap Buffer Overflow in dcmqrscp | **Closed** | **2026-05-04** |

### History

**#1 - 2026-04-02 23:43 - Jörg Riesmeier**

*- Description updated*

**#2 - 2026-05-06 19:34 - Marco Eichelberg**

*- Status changed from New to Closed*

*- % Done changed from 0 to 100*

This issue was apparently logged twice. See issue 1206: http://support.dcmtk.org/redmine/issues/1206

**#3 - 2026-05-06 19:37 - Jörg Riesmeier**

*- Has duplicate Bug #1206: Remote Heap Buffer Overflow in dcmqrscp added*

**#4 - 2026-05-22 09:30 - Marco Eichelberg**

*- Private changed from Yes to No*

### Files

| | | | |
|---|---|---|---|
| dcmqrscp.cfg | 321 Bytes | 2026-04-02 | Jörg Riesmeier |
| template.dcm | 522 Bytes | 2026-04-02 | Jörg Riesmeier |
| valgrind_report_1.txt | 19.3 KB | 2026-04-02 | Jörg Riesmeier |
| valgrind_report2.txt | 14.4 KB | 2026-04-02 | Jörg Riesmeier |