



Heap Buffer Overflow in DICOM Image Decoder via VR UL Dimensions

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-5442
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 15:16:16 UTC
Updated	2026-04-14 20:19:46 UTC

Description A heap buffer overflow vulnerability exists in the DICOM image decoder. Dimension fields are encoded using Value Repres

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from ADP

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000170000 probability, percentile 0.038940000 (date 2026-04-14)

Problem Types: CWE-787 | CWE-190 Integer Overflow or Wraparound

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

High
 Integrity
 High
 Availability
 High
 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Orthanc-server	Orthanc	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Orthanc	DICOM Server	affected 1.12.10 custom	Not specified

References

Reference	Source	Link	Tags
kb.cert.org/vuls/id/536588	cret@cert.org	kb.cert.org	Third Party Advisory, VDB Entry
www.orthanc-server.com	cret@cert.org	www.orthanc-server.com	Product
www.machinespirits.de	cret@cert.org	www.machinespirits.de	Not Applicable
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.