



Heap Buffer Overflow in PAM Image Buffer Allocation

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

Summary

CVE	CVE-2026-5444
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 20:20:10 UTC
Description	A heap buffer overflow vulnerability exists in the PAM image parsing logic. When Orthanc processes a crafted PAM image e

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from ADP

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

EPSS: 0.000190000 probability, percentile 0.049970000 (date 2026-04-14)

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

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

High

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report