



HDF5 H5Fint.c H5F_addr_decode_len heap-based overflow

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

Summary

CVE	CVE-2025-6516
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-23 17:15:32 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability has been found in HDF5 up to 1.14.6 and classified as critical. This vulnerability affects the function H5F_addr_decode_len in heap-based memory. The vulnerability allows an attacker to overflow the heap, leading to memory corruption and potential denial of service or remote code execution.

Risk And Classification

Primary CVSS: v4.0 1.9 LOW from cna@vulldb.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-119 | CWE-122 | CWE-787 | CWE-122 Heap-based Buffer Overflow | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vulldb.com	Secondary	1.9	LOW	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vulldb.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	5.3	MEDIUM	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
2.0	cna@vulldb.com	Secondary	4.3	MEDIUM	AV:L/AC:L/Au:S/C:P/I:P/A:P
2.0	CNA	DECLARED	4.3	MEDIUM	AV:L/AC:L/Au:S/C:P/I:P/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hdfgroup	Hdf5	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	HDF5	affected 1.14.0	Not specified
CNA	Na	HDF5	affected 1.14.1	Not specified
CNA	Na	HDF5	affected 1.14.2	Not specified
CNA	Na	HDF5	affected 1.14.3	Not specified
CNA	Na	HDF5	affected 1.14.4	Not specified
CNA	Na	HDF5	affected 1.14.5	Not specified
CNA	Na	HDF5	affected 1.14.6	Not specified

References

Reference	Source	Link	Tags
github.com/user-attachments/files/20626851/reproduce.tar.gz	cna@vuldb.com	github.com	Exploit
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisory, VDB Entry
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisory, VDB Entry
github.com/HDFGroup/hdf5/issues/5581	cna@vuldb.com	github.com	Exploit, Issue Tracking, Third Party Advisor
vuldb.com	cna@vuldb.com	vuldb.com	Permissions Required, VDB Entry
CVE Program record	CVE ORG	www.cve.org	canonical

CVE Program Home CVE IDs www.cve.org canonical

NVD vulnerability detail NVD nvd.nist.gov canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Rulkallos (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-06-23T00:00:00.000Z	Advisory disclosed
CNA	2025-06-23T02:00:00.000Z	VulDB entry created
CNA	2025-06-23T14:23:40.000Z	VulDB entry last update

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

© [CVE.report](http://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