



NASA cFS CCSDS Packet Header to_lab_passthru_encode.c CFE_MSG_GetSize heap- based overflow

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

Summary

CVE	CVE-2026-5474
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-03 17:16:54 UTC
Updated	2026-04-03 17:16:54 UTC
Description	A vulnerability was found in NASA cFS up to 7.0.0. This affects the function CFE_MSG_GetSize of the file apps/to_lab/fsw/

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from cna@vuldb.com

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:X/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-122 Heap-based Buffer Overflow | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	5.3	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:X/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	5.3	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:X/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	cna@vuldb.com	Primary	6.3	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	6.3	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:X/RL:X/RC:R
3.0	CNA	DECLARED	6.3	MEDIUM	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:X/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	5.8		AV:A/AC:L/Au:N/C:P/I:P/A:P
2.0	CNA	DECLARED	5.8		AV:A/AC:L/Au:N/C:P/I:P/A:P/E:ND/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:X/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

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

CVSS v3.0 Breakdown

Attack Vector

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	NASA	CFS	affected 7.0	Not specified

References

Reference	Source	Link	Tags
vuldb.com/submit/781950	cna@vuldb.com	vuldb.com	
github.com/nasa/cFS	cna@vuldb.com	github.com	
vuldb.com/vuln/355078	cna@vuldb.com	vuldb.com	
vuldb.com/vuln/355078/cti	cna@vuldb.com	vuldb.com	
github.com/nasa/cFS/issues/952	cna@vuldb.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: OrbitingZero (VulDB User) (en)

CNA: VulDB CNA Team (en)

Additional Advisory Data

Source	Time	Event
--------	------	-------

CNA	2026-04-03T00:00:00.000Z	Advisory disclosed
CNA	2026-04-03T02:00:00.000Z	VulDB entry created
CNA	2026-04-03T09:56:30.000Z	VulDB entry last update

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)