Ffmpeg: null pointer dereference in ffmpeg als decoder (libavcodec/alsdec.c)

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-7700
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-11-07 19:16:27 UTC
Updated	2026-05-06 16:16:04 UTC
Description	A flaw was found in FFmpeg's ALS audio decoder, where it does not properly check for memory allocation failures. This ca

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from secalert@redhat.com

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

Problem Types: CWE-476 | CWE-476 NULL Pointer Dereference

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
None

Integrity
None

Availability

Low

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

There are no known software configurations currently associated with this CVE in NVD or the CVE Program record.

References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
github.com/FFmpeg/FFmpeg/commit/35a6de137a39f274d5e01ed0e0e6c4f04d0aaf07	secalert@redhat.com	github.com	
access.redhat.com/security/cve/CVE-2025-7700	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Jiasheng Jiang for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-07-16T04:55:06.900Z	Reported to Red Hat.
CNA	2025-07-15T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability. Users are strongly encouraged to apply vendor-supplied updates or patches as they become available to address this vulnerability.

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

Free CVE JSON API cve.report/api

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