Ffmpeg: ffmpeg: denial of service and potential arbitrary code execution via signed integer overflow in dvd subtitle parser

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

Summary

CVE	CVE-2026-6385
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 20:16:44 UTC
Updated	2026-04-17 15:17:00 UTC
Description	A flaw was found in FFmpeg. A remote attacker could exploit this vulnerability by providing a specially crafted MPEG-PS/V(

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from secalert@redhat.com

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

EPSS: 0.000710000 probability, percentile 0.217860000 (date 2026-04-21)

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

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Lightspeed Core	Not specified	Not specified
CNA	Red Hat	Red Hat AI Inference Server	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux AI RHEL AI 3	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux AI RHEL AI 3	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux AI RHEL AI 3	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux AI RHEL AI 3	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux AI RHEL AI 3	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux AI RHEL AI 3	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift AI RHOAI	Not specified	Not specified

References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-6385	secalert@redhat.com	access.redhat.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: Red Hat would like to thank Quang Luong (Calif.io in collaboration with OpenAI Codex) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-15T19:11:15.167Z	Reported to Red Hat.
CNA	2026-04-15T19:11:47.803Z	Made public.

Workarounds

CNA: To mitigate this issue, avoid processing untrusted MPEG-PS/VOB media files with FFmpeg. If FFmpeg is used in automated media processing services, implement strict input validation and isolation to prevent the ingestion of malicious files from untrusted sources. For end-user applications, refrain from opening or playing untrusted media files.

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