



# 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

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

## 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

Integrity

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 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	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
access.redhat.com/security/cve/CVE-2026-6385	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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.

© [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](#)