



CVE-2021-30145

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

Summary

CVE	CVE-2021-30145
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-18 14:15:00 UTC
Updated	2022-05-20 20:45:00 UTC
Description	A format string vulnerability in mpv through 0.33.0 allows user-assisted remote attackers to achieve code execution via a cr

Risk And Classification

Problem Types: CWE-134

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mpv	Mpv	All	All	All	All

References

Reference	Source	Link	Tags
mpv: Format string vulnerability (GLSA 202107-46) — Gentoo security	GENTOO	security.gentoo.org	
demux_mf: improve format string processing · mpv-player/mpv@d0c5309 · GitHub	MISC	github.com	
mpv media player – mf custom protocol vulnerability (CVE-2021-30145) – development.de	MISC	development.de	
Release v0.33.1 · mpv-player/mpv · GitHub	MISC	github.com	
mpv.io	MISC	mpv.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180597](#) Debian Security Update for mpv (CVE-2021-30145)

[501626](#) Alpine Linux Security Update for mpv

710023 Gentoo Linux mpv Format string vulnerability (GLSA 202107-46)
750192 OpenSUSE Security Update for mpv (openSUSE-SU-2021:0788-1)

© [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](#)