



CVE-2020-36133

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

Summary

CVE	CVE-2020-36133
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-02 22:15:00 UTC
Updated	2024-01-31 15:15:00 UTC
Description	AOM v2.0.1 was discovered to contain a global buffer overflow via the component av1/encoder/partition_search.h.

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Aomedia	Aomedia	2.0.1	All	All	All

References

Reference	Source	Link
libaom: Multiple Vulnerabilities (GLSA 202401-32) — Gentoo security		security.gentoo.org
2913 - aomedia - The open and royalty-free codec for next-generation ultra high definition media - Monorail	MISC	bugs.chromium.org
[SECURITY] [DLA 3556-1] aom security update	MLIST	lists.debian.org
Debian -- Security Information -- DSA-5490-1 aom	DEBIAN	www.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

199852 Ubuntu Security Notification for AOM Vulnerabilities (USN-6447-1)
6000110 Debian Security Update for aom (DLA 3556-1)
6000224 Debian Security Update for aom (DSA 5490-1)

© [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](#).

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