



CVE-2023-44488

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

Summary

CVE	CVE-2023-44488
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-30 20:15:00 UTC
Updated	2023-11-16 01:37:00 UTC
Description	VP9 in libvpx before 1.13.1 mishandles widths, leading to a crash related to encoding.

Risk And Classification

Problem Types: CWE-755

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	12.0	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Webmproject	Libvpx	All	All	All	All

References

Reference
Fix bug with smaller width bigger size · webmproject/libvpx@263682c · GitHub
[SECURITY] [DLA 3598-1] libvpx security update
[SECURITY] Fedora 37 Update: libvpx-1.12.0-4.fc37 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 37 Update: libvpx-1.12.0-4.fc37 - package-announce - Fedora Mailing-Lists
Comparing v1.13.0...v1.13.1 · webmproject/libvpx · GitHub
Debian -- Security Information -- DSA-5518-1 libvpx
2241806 – (CVE-2023-44488, TRIAGE-CVE-2023-44488) CVE-2023-44488 TRIAGE-CVE-2023-44488 libvpx: crash related to VP9 encoding
libvpx: Multiple Vulnerabilities (CVE SA 202310 04) - Gentoo security

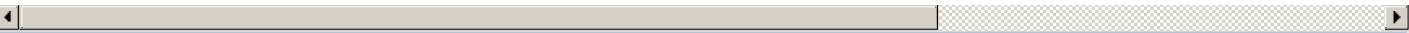
[Fix bug with smaller width bigger size · webmproject/libvpx@df9fd9d · GitHub](#)

[oss-security - Re: CVE-2023-5217: Heap buffer overflow in vp8 encoding in libvpx](#)

[Release v1.13.1: libvpx 1.13.1 · webmproject/libvpx · GitHub](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160966](#) Oracle Enterprise Linux Security Update for libvpx (ELSA-2023-5537)

[160970](#) Oracle Enterprise Linux Security Update for libvpx (ELSA-2023-5539)

[161029](#) Oracle Enterprise Linux Security Update for firefox (ELSA-2023-6162)

[161033](#) Oracle Enterprise Linux Security Update for firefox (ELSA-2023-6187)

[161034](#) Oracle Enterprise Linux Security Update for thunderbird (ELSA-2023-6191)

[161035](#) Oracle Enterprise Linux Security Update for thunderbird (ELSA-2023-6194)

[161036](#) Oracle Enterprise Linux Security Update for thunderbird (ELSA-2023-6193)

[161037](#) Oracle Enterprise Linux Security Update for firefox (ELSA-2023-6188)

[199793](#) Ubuntu Security Notification for libvpx Vulnerabilities (USN-6403-1)

[199850](#) Ubuntu Security Notification for libvpx Vulnerabilities (USN-6403-2)

[199885](#) Ubuntu Security Notification for libvpx Vulnerabilities (USN-6403-3)

[242128](#) Red Hat Update for libvpx (RHSA-2023:5535)

[242129](#) Red Hat Update for libvpx (RHSA-2023:5534)

[242135](#) Red Hat Update for libvpx (RHSA-2023:5536)

[242136](#) Red Hat Update for libvpx (RHSA-2023:5538)

[242137](#) Red Hat Update for libvpx (RHSA-2023:5537)

[242138](#) Red Hat Update for libvpx (RHSA-2023:5539)

[242139](#) Red Hat Update for libvpx (RHSA-2023:5540)

[242247](#) Red Hat Update for firefox (RHSA-2023:6162)

[242249](#) Red Hat Update for thunderbird (RHSA-2023:6198)

[242250](#) Red Hat Update for firefox (RHSA-2023:6189)

242251 Red Hat Update for thunderbird (RHSA-2023:6197)
242252 Red Hat Update for firefox (RHSA-2023:6190)
242253 Red Hat Update for firefox (RHSA-2023:6188)
242254 Red Hat Update for firefox (RHSA-2023:6186)
242255 Red Hat Update for firefox (RHSA-2023:6185)
242257 Red Hat Update for thunderbird (RHSA-2023:6196)
242258 Red Hat Update for firefox (RHSA-2023:6199)
242259 Red Hat Update for thunderbird (RHSA-2023:6195)
242355 Red Hat Update for thunderbird (RHSA-2023:6194)
242366 Red Hat Update for thunderbird (RHSA-2023:6192)
242368 Red Hat Update for firefox (RHSA-2023:6187)
242397 Red Hat Update for thunderbird (RHSA-2023:6191)
284655 Fedora Security Update for libvpx (FEDORA-2023-f696934fbf)
296105 Oracle Solaris 11.4 Support Repository Update (SRU) 63.157.1 Missing (CPUOCT2023)
356441 Amazon Linux Security Advisory for thunderbird : ALAS2-2023-2294
356607 Amazon Linux Security Advisory for firefox : ALAS2FIREFOX-2023-016
356629 Amazon Linux Security Advisory for libvpx : ALAS2023-2023-413
378965 Alibaba Cloud Linux Security Update for libvpx (ALINUX3-SA-2023:0129)
6000146 Debian Security Update for libvpx (DLA 3598-1)
6000214 Debian Security Update for libvpx (DSA 5518-1)
673948 EulerOS Security Update for libvpx (EulerOS-SA-2024-1279)
710763 Gentoo Linux libvpx Multiple Vulnerabilities (GLSA 202310-04)
907551 Common Base Linux Mariner (CBL-Mariner) Security Update for libvpx (30066-1)
941289 AlmaLinux Security Update for libvpx (ALSA-2023:5537)
941290 AlmaLinux Security Update for libvpx (ALSA-2023:5539)
941333 AlmaLinux Security Update for thunderbird (ALSA-2023:6191)
941334 AlmaLinux Security Update for firefox (ALSA-2023:6188)
941341 AlmaLinux Security Update for firefox (ALSA-2023:6187)

941343 AlmaLinux Security Update for thunderbird (ALSA-2023:6194)

961069 Rocky Linux Security Update for firefox (RLSA-2023:6188)

© [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](#)