



CVE-2023-45853

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-45853
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-14 02:15:00 UTC
Updated	2024-01-24 21:15:00 UTC
Description	MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_64 v

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
[debian-lts-announce] 20231127 [SECURITY] [DLA 3670-1] minizip security update
zlib: Buffer Overflow (GLSA 202401-18) — Gentoo security
pyminizip · PyPI
security.netapp.com/advisory/ntap-20231130-0009
minizip: Check length of comment, filename, and extra field, in zipOpenNewFileInZip4_64 by zmodem · Pull Request #843 · madler/zlib · GitHub
oss-security - CVE-2023-45853: overflows in MiniZip in zlib through 1.3
Minizip: Zip and UnZip additional library
github.com/madler/zlib/blob/ac8f12c97d1afd9bafa9c710f827d40a407d3266/con...
d709fb23806858847131027da95ef4c548813356 - chromium/src - Git at Google
de29dd6c7151d3cd37cb4cf0036800ddfb1d8b61 - chromium/src - Git at Google
oss-security - Re: CVE-2023-45853: overflows in MiniZip in zlib through 1.3
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[356563](#) Amazon Linux Security Advisory for zlib : ALAS2-2023-2320

[356623](#) Amazon Linux Security Advisory for zlib : ALAS2023-2023-410

[503434](#) Alpine Linux Security Update for minizip

[503480](#) Alpine Linux Security Update for qt5-qtwebengine

[506117](#) Alpine Linux Security Update for minizip

[506204](#) Alpine Linux Security Update for qt5-qtwebengine

[506211](#) Alpine Linux Security Update for qt6-qtwebengine

[6000355](#) Debian Security Update for minizip (DLA 3670-1)

[673334](#) EulerOS Security Update for binutils (EulerOS-SA-2023-3236)

[673385](#) EulerOS Security Update for zlib (EulerOS-SA-2024-1170)

[673387](#) EulerOS Security Update for binutils (EulerOS-SA-2024-1078)

[673408](#) EulerOS Security Update for zlib (EulerOS-SA-2023-3353)

[673447](#) EulerOS Security Update for zlib (EulerOS-SA-2023-3321)

[673507](#) EulerOS Security Update for binutils (EulerOS-SA-2024-1054)

[673545](#) EulerOS Security Update for binutils (EulerOS-SA-2023-3292)

[673661](#) EulerOS Security Update for zlib (EulerOS-SA-2023-3261)

[673799](#) EulerOS Security Update for binutils (EulerOS-SA-2024-1257)

[673842](#) EulerOS Security Update for binutils (EulerOS-SA-2023-3324)

[673875](#) EulerOS Security Update for binutils (EulerOS-SA-2024-1133)

[673886](#) EulerOS Security Update for binutils (EulerOS-SA-2023-3264)

[673896](#) EulerOS Security Update for zlib (EulerOS-SA-2024-1100)

[673965](#) EulerOS Security Update for zlib (EulerOS-SA-2024-1076)

[674078](#) EulerOS Security Update for zlib (EulerOS-SA-2024-1308)

[674080](#) EulerOS Security Update for zlib (EulerOS-SA-2023-3289)

[710837](#) Gentoo Linux zlib Buffer Overflow Vulnerability (GLSA 202401-18)

755158 SUSE Enterprise Linux Security Update for zlib (SUSE-SU-2023:4217-1)
755159 SUSE Enterprise Linux Security Update for zlib (SUSE-SU-2023:4216-1)
755160 SUSE Enterprise Linux Security Update for zlib (SUSE-SU-2023:4215-1)
907483 Common Base Linux Mariner (CBL-Mariner) Security Update for zlib (31500)
907500 Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (31298-1)
907506 Common Base Linux Mariner (CBL-Mariner) Security Update for boost (31294-1)
907509 Common Base Linux Mariner (CBL-Mariner) Security Update for tcl (31497-1)
907523 Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (31298-2)
907571 Common Base Linux Mariner (CBL-Mariner) Security Update for zlib (31500-1)
907832 Common Base Linux Mariner (CBL-Mariner) Security Update for rubygem-mini_portile2 (33350-2)
996366 Python (Pip) Security Update for pyminizip (GHSA-mq29-j5xf-cjwr)

© [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](#)