



CVE-2017-14107

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

Summary

CVE	CVE-2017-14107
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-01 17:29:00 UTC
Updated	2022-04-06 18:35:00 UTC
Description	The _zip_read_eocd64 function in zip_open.c in libzip before 1.3.0 mishandles EOCD records, which allows remote attackers

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Libzip	Libzip	All	All	All	All
Application	Libzip	Libzip	All	All	All	All

References

Reference	Source	Link	Tags
libzip: memory allocation failure in _zip_cdir_grow (zip_dirent.c) agostino's blog	MISC	blogs.gentoo.org	Patch, Vulnerability
[SECURITY] [DLA 2858-1] libzip security update	MLIST	lists.debian.org	
Make eocd checks more consistent between zip and zip64 cases. · nih-at/libzip@9b46957 · GitHub	MISC	github.com	Issue T
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178961](#) Debian Security Update for libzip (DLA 2858-1)

[501071](#) Alpine Linux Security Update for libzip

© [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](#)