



CVE-2020-18442

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

Summary

CVE	CVE-2020-18442
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-18 15:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	Infinite Loop in zziplib v0.13.69 allows remote attackers to cause a denial of service via the return value "zzip_file_read" in t

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Zziplib Project	Zziplib	0.13.69	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora 34 Update: zziplib-0.13.72-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 35 Update: zziplib-0.13.72-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Ma
[SECURITY] [DLA 2859-1] zziplib security update	MLIST	lists.debian.org	
[SECURITY] Fedora 35 Update: zziplib-0.13.72-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
error: Incorrect handling of function 'zzip_fread' return value · Issue #68 · gdraheim/zziplib · GitHub	MISC	github.com	
[SECURITY] Fedora 34 Update: zziplib-0.13.72-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Ma
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159485](#) Oracle Enterprise Linux Security Update for zziplib (ELSA-2021-4316)

[178959](#) Debian Security Update for zziplib (DLA 2859-1)

[199666](#) Ubuntu Security Notification for ZZIPLib Vulnerabilities (USN-6298-1)

[239792](#) Red Hat Update for zziplib (RHSA-2021:4316)

[282400](#) Fedora Security Update for zziplib (FEDORA-2022-8109b472a3)

[282401](#) Fedora Security Update for zziplib (FEDORA-2022-737e44718a)

[354268](#) Amazon Linux Security Advisory for zziplib : ALAS2022-2022-162

[354442](#) Amazon Linux Security Advisory for zziplib : ALAS2022-2022-081

[355153](#) Amazon Linux Security Advisory for zziplib : ALAS2023-2023-006

[670733](#) EulerOS Security Update for zziplib (EulerOS-SA-2021-2491)

[750721](#) SUSE Enterprise Linux Security Update for zziplib (SUSE-SU-2021:2164-1)

[755993](#) SUSE Enterprise Linux Security Update for zziplib (SUSE-SU-2024:0970-1)

[940283](#) AlmaLinux Security Update for zziplib (ALSA-2021:4316)

[960254](#) Rocky Linux Security Update for zziplib (RLSA-2021:4316)

© [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](#)