



CVE-2022-28044

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

Summary

CVE	CVE-2022-28044
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-15 14:15:00 UTC
Updated	2022-07-22 09:47:00 UTC
Description	lrzip v0.640 was discovered to contain a heap memory corruption via the component lrzip.c:initialise_control.

Risk And Classification

Problem Types: CWE-787

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	9.0	All	All	All
Application	lrzip Project	lrzip	0.640	All	All	All

References

Reference	Source	Link
Fix control->suffix being deallocated as heap memory as reported by P... · ckolivas/lrzip@5faf80c · GitHub	MISC	github.com
Debian -- Security Information -- DSA-5145-1 lrzip	DEBIAN	www.debian.org
Deallocation of control->suffix corrupts Heap Memory · Issue #216 · ckolivas/lrzip · GitHub	MISC	github.com
[SECURITY] [DLA 3005-1] lrzip security update	MLIST	lists.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

179284 Debian Security Update for Irzip (DLA 3005-1)
179313 Debian Security Update for Irzip (DSA 5145-1)
182986 Debian Security Update for Irzip (CVE-2022-28044)
199146 Ubuntu Security Notification for Long Range ZIP Vulnerabilities (USN-5840-1)
502884 Alpine Linux Security Update for Irzip
505763 Alpine Linux Security Update for Irzip

© [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](#)