



CVE-2019-14866

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

Summary

CVE	CVE-2019-14866
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-07 17:15:00 UTC
Updated	2023-06-04 22:15:00 UTC
Description	In all versions of cpio before 2.13 does not properly validate input files when generating TAR archives. When cpio is used to

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Cpio	All	All	All	All
Application	Gnu	Cpio	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference
[SECURITY] [DLA 3445-1] cpio security update
1765511 – (CVE-2019-14866) CVE-2019-14866 cpio: improper input validation when writing tar header fields leads to unexpect tar generation
Red Hat Customer Portal - Access to 24x7 support and knowledge
[Bug-cpio] [PATCH] Check for size overflow in tar header fields
1765511 – (CVE-2019-14866) CVE-2019-14866 cpio: improper input validation when writing tar header fields leads to unexpect tar generation
Red Hat Customer Portal - Access to 24x7 support and knowledge
Red Hat Customer Portal - Access to 24x7 support and knowledge
cpio-2.13 released [stable]

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159187](#) Oracle Enterprise Linux Security Update for cpio (ELSA-2021-1582)

[181827](#) Debian Security Update for cpio (DLA 3445-1)

[239337](#) Red Hat Update for cpio (RHSA-2021:1582)

[239988](#) Red Hat Update for cpio (RHSA-2022:0073)

[377503](#) Alibaba Cloud Linux Security Update for cpio (ALINUX2-SA-2020:0131)

[500862](#) Alpine Linux Security Update for cpio

[504655](#) Alpine Linux Security Update for cpio

[940193](#) AlmaLinux Security Update for cpio (ALSA-2021:1582)

[960855](#) Rocky Linux Security Update for cpio (RLSA-2021:1582)

© [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](#)