



CVE-2014-9112

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

Summary

CVE	CVE-2014-9112
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-02 16:59:00 UTC
Updated	2017-09-08 01:29:00 UTC
Description	Heap-based buffer overflow in the process_copy_in function in GNU Cpio 2.11 allows remote attackers to cause a denial of

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Gnu	Cpio	2.11	All	All	All
Application	Gnu	Cpio	2.11	All	All	All

References

Reference

GNU cpio - Bugs: bug #43709, Out-of-bounds write in... [Savannah]
IBM X-Force Exchange
oss-security - so, can we do something about lesspipe? (+ a cpio bug to back up the argument)
Linux Kernel cpio 'list_file()' Function Heap Based Buffer Overflow Vulnerability
About Secunia Research Flexera
Security Advisory SA60167 - GNU Cpio Archive Handling Vulnerabilities - Secunia
Oracle Linux Bulletin - October 2015
Debian -- Security Information -- DSA-3111-1 cpio
oss-security - CVE request: cpio heap-based buffer overflow [was Re: so, can we do something about lesspipe? (+ a cpio bug to back up the e
Full Disclosure: on Linux, 'less' can probably get you owned

oss-security - Re: CVE request: cpio heap-based buffer overflow [was Re: so, can we do something about lesspipe? (+ a cpio bug to back up

USN-2456-1: GNU cpio vulnerabilities | Ubuntu

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)