



# CVE-2021-33640

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

## Summary

<b>CVE</b>	CVE-2021-33640
<b>State</b>	PUBLIC
<b>Assigner</b>	securities@openeuler.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-12-19 16:15:00 UTC
<b>Updated</b>	2023-11-07 03:35:00 UTC
<b>Description</b>	After tar_close(), libtar.c releases the memory pointed to by pointer t. After tar_close() is called in the list() function, it contin

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Huawei</a>	<a href="#">Openeuler</a>	20.03	sp1	All	All
Operating System	<a href="#">Huawei</a>	<a href="#">Openeuler</a>	20.03	sp2	All	All
Operating System	<a href="#">Huawei</a>	<a href="#">Openeuler</a>	22.03	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] Fedora 36 Update: libtar-1.2.20-26.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 37 Update: libtar-1.2.20-26.fc37 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 36 Update: libtar-1.2.20-26.fc36 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 37 Update: libtar-1.2.20-26.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
CVE Detail	MISC	<a href="https://www.openeuler.org">www.openeuler.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	cano
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	cano

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">283563</a> Fedora Security Update for libtar (FEDORA-2022-ccc68b06cc)
<a href="#">283564</a> Fedora Security Update for libtar (FEDORA-2022-88772d0a2d)
<a href="#">672599</a> EulerOS Security Update for libtar (EulerOS-SA-2023-1324)
<a href="#">672709</a> EulerOS Security Update for libtar (EulerOS-SA-2023-1448)
<a href="#">672751</a> EulerOS Security Update for libtar (EulerOS-SA-2023-1473)
<a href="#">672797</a> EulerOS Security Update for libtar (EulerOS-SA-2023-1529)
<a href="#">672804</a> EulerOS Security Update for libtar (EulerOS-SA-2023-1554)
<a href="#">672850</a> EulerOS Security Update for libtar (EulerOS-SA-2023-1575)
<a href="#">672854</a> EulerOS Security Update for libtar (EulerOS-SA-2023-1585)
<a href="#">904891</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libtar (12359)
<a href="#">905158</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libtar (12519)
<a href="#">905191</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libtar (12909)
<a href="#">905226</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libtar (12933)
<a href="#">905410</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libtar (12933-1)
<a href="#">905480</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libtar (12909-1)

© [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](#)