



CVE-2021-31272

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

Summary

CVE	CVE-2021-31272
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-18 22:15:00 UTC
Updated	2021-06-22 17:03:00 UTC
Description	SerenityOS before commit 3844e8569689dd476064a0759d704bc64fb3ca2c contains a directory traversal vulnerability in tar

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Serenityos	Serenityos	All	All	All	All

References

Reference	Source
Userland: Fix tar/unzip directory traversal vulnerability by bblenard · Pull Request #5713 · SerenityOS/serenity · GitHub	MITRE
unzip: Directory traversal vulnerability may lead to command execution / privilege escalation · Issue #3992 · SerenityOS/serenity · GitHub	MITRE
Userland: Fix tar/unzip directory traversal vulnerability by bblenard · Pull Request #5713 · SerenityOS/serenity · GitHub	CVE
tar: Directory traversal vulnerability may lead to command execution / privilege escalation · Issue #3991 · SerenityOS/serenity · GitHub	MITRE
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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