



CVE-2021-41072

Published on: 09/13/2021 12:00:00 AM UTC

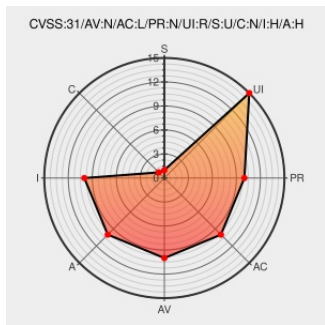
Last Modified on: 10/15/2021 08:15:00 PM UTC

CVE-2021-41072

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of [Squashfs-tools](#) from [Squashfs-tools Project](#) contain the following vulnerability:

squashfs_opendir in unsquash-2.c in Squashfs-Tools 4.5 allows Directory Traversal, a different vulnerability than CVE-2021-40153. A squashfs filesystem that has been crafted to include a symbolic link and then contents under the same filename in a filesystem can cause unsquashfs to first create the symbolic link pointing outside the expected directory, and then the subsequent write operation will cause the unsquashfs process to write through the symbolic link elsewhere in the filesystem.

CVE-2021-41072 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	HIGH

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
unsquashfs - unvalidated filename allow writing outside		MISC github.com/dlouchet/squashfs

unsquashfs - unvalidated heaptrails allow writing outside of destination · Issue #72 · plougher/squashfs-tools · GitHub

[github.com](#)
[text/html](#)

MISC github.com/plougher/squashfs-tools/issues/72#issuecomment-913833405

Unsquashfs: additional write outside destination directory exploit fix · plougher/squashfs-tools@e048580 · GitHub

[github.com](#)
[text/html](#)

MISC github.com/plougher/squashfs-tools/commit/e0485802ec72996c20026da320650d8362f555bd

Debian -- Security Information -- DSA-4987-1 squashfs-tools

www.debian.org
[Deprecated Link](#)
[text/html](#)

DEBIAN [DSA-4987](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[198500](#) Ubuntu Security Notification for Squashfs-Tools Vulnerability (USN-5078-1)

[198537](#) Ubuntu Security Notification for Squashfs-Tools Vulnerability (USN-5078-3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Squashfs-tools Project	Squashfs-tools	4.5	All	All	All

cpe:2.3:a:squashfs-tools_project:squashfs-tools:4.5:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41072 : squashfs_opendir in unsquash-2.c in Squashfs-Tools 4.5 allows Directory Traversal, a different vul... twitter.com/i/web/status/1...	2021-09-14 01:04:39

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2021 [T](#) [N](#) |

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](#)