



CVE-2023-28101

Published on: Not Yet Published

Last Modified on: 03/22/2023 07:02:00 PM UTC

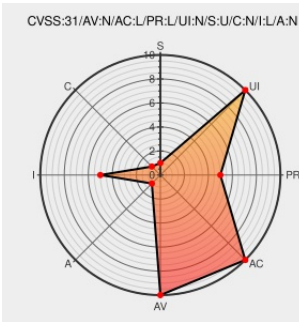
CVE-2023-28101 - advisory for GHSA-h43h-fwqx-mpp8

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of Flatpak from Flatpak contain the following vulnerability:

Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4, if an attacker publishes a Flatpak app with elevated permissions, they can hide those permissions from users of the `flatpak(1)` command-line interface by setting other permissions to crafted values that contain non-printable control characters such as `ESC`. A fix is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, use a GUI like GNOME Software rather than the command-line interface, or only install apps whose maintainers you trust.

CVE-2023-28101 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: flatpak - flatpak version = < 1.10.8

Affected Vendor/Software: flatpak - flatpak version = >= 1.12.0, < 1.12.8

Affected Vendor/Software: flatpak - flatpak version = >= 1.14.0, < 1.14.4

Affected Vendor/Software: flatpak - flatpak version = >= 1.15.0, < 1.15.4

CVSS3 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Reject paths given to --filesystem/--persist with special characters · flatpak/flatpak@7fe63f2 · GitHub	github.com text/html	MISC github.com/flatpak/flatpak/commit/7fe63f2e8f1fd2dafc31d45154cf0b191ebec66c
CVE-2023-28101: Metadata with ANSI control codes can cause misleading terminal output · Advisory · flatpak/flatpak · GitHub	github.com text/html	MISC github.com/flatpak/flatpak/security/advisories/GHSA-h43h-fwqx-mpp8
cli-transaction: Escape any special characters in the EOL reason · flatpak/flatpak@409e341 · GitHub	github.com text/html	MISC github.com/flatpak/flatpak/commit/409e34187de2b2b2c4ef34c79f417be698830f6c
Ensure special characters in permissions and metadata are escaped · flatpak/flatpak@6cac99d · GitHub	github.com text/html	MISC github.com/flatpak/flatpak/commit/6cac99dfe6003c8a4bd5666341c217876536869

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

- [181854](#) Debian Security Update for flatpak (CVE-2023-28101)
- [283814](#) Fedora Security Update for flatpak (FEDORA-2023-b0717d8c45)
- [283849](#) Fedora Security Update for flatpak (FEDORA-2023-9fbc701e0d)
- [284241](#) Fedora Security Update for flatpak (FEDORA-2023-508e400dec)
- [753858](#) SUSE Enterprise Linux Security Update for flatpak (SUSE-SU-2023:1714-1)
- [753859](#) SUSE Enterprise Linux Security Update for flatpak (SUSE-SU-2023:1713-1)
- [753883](#) SUSE Enterprise Linux Security Update for flatpak (SUSE-SU-2023:1712-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Flatpak	Flatpak	All	All	All	All
<code>cpe:2.3:a:flatpak:flatpak:*:*:*:*:*:*</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-28101 : Flatpak is a system for building, distributing, and running sandboxed desktop applications on... twitter.com/i/web/status/1...	2023-03-16 16:01:34
@FlatpakApps	One issue (CVE-2023-28101) involves maliciously crafted metadata hiding permissions using special characters and th... twitter.com/i/web/status/1...	2023-03-16 19:22:41
/r/netcve	CVE-2023-28101	2023-03-16

[← Previous ID](#)[Next ID→](#)

© CVE.report 2023   |

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](#)