

[Products](#)[Services](#)[Publications](#)[Resources](#)[What's new](#)

[Follow @Openwall on Twitter for new release announcements and other news](#)

[\[<prev\]](#) [\[next>\]](#) [\[day\]](#) [\[month\]](#) [\[year\]](#) [\[list\]](#)

Message-ID: <admDB8Eiz6MGYYu0@definition.pseudorandom.co.uk>  
Date: Sat, 11 Apr 2026 00:08:55 +0100  
From: Simon McVittie <smcv@...ian.org>  
To: oss-security@...ts.openwall.com  
Subject: xdg-desktop-portal GHSA-rqr9-jwwf-wxgj: Trashing of arbitrary host files

xdg-desktop-portal's Trash portal is designed to allow sandboxed apps to ask for a file or directory accessible to the app to be moved to the trash.

Similar to CVE-2026-34078 in Flatpak (but less serious), Codean Labs reported that a malicious or compromised Flatpak app could ask the portal to trash a file that it owns, then replace that file with a symlink, exploit a time-of-check/time-of-use mismatch and make the portal trash the target of the symlink on the host system instead.

This is fixed in stable release 1.20.4 and development prerelease 1.21.1.

<https://github.com/flatpak/xdg-desktop-portal/security/advisories/GHSA-rqr9-jwwf-wxgj>

[Powered by blists - more mailing lists](#)

Please check out the [Open Source Software Security Wiki](#), which is counterpart to this [mailing list](#).

Confused about [mailing lists](#) and their use? [Read about mailing lists on Wikipedia](#) and check out these [guidelines on proper formatting of your messages](#).