Flatpak Sandbox Escape via Yelp

May 11, 2026

Fedora, GNOME, Security

Yelp 49.1 fixes a significant Flatpak sandbox escape related to last year's CVE-2025-3155. CVE assignment for this new issue is currently pending. **June 29, 2026 update:** better late than never, we have received CVE-2026-13601.

This is not a bug in Flatpak. Flatpak allows sandboxed applications to open URIs or files, meaning the sandboxed application may use a URI or file path to launch another application to open the URI or file. This is brokered via the OpenURI portal. The portal or the app may decide to require user interaction to decide which app to launch, but user interaction is generally not required. This is necessary: you would get pretty frustrated if you were prompted to select which app to use every time you click on a link or try to open something! Accordingly, unsandboxed applications that are installed on the host system are somewhat risky: any malicious sandboxed app may launch an unsandboxed app using a malicious file, generally with no user interaction required. Unsandboxed applications installed on the host OS are inherently part of the attack surface of the Flatpak sandbox.

In this case, a sandboxed application may launch Yelp to open a malicious help file. The help file can then exfiltrate arbitrary files from your host OS to a web server by using a CSS stylesheet embedded in an SVG. Suffice to say the attack is pretty

clever, and certainly more impactful than the typical boring memory safety bugs I more commonly see.

This bug was discovered by Codean Labs, which performed a security audit of Flatpak and several GNOME projects thanks to generous sponsorship by the Sovereign Tech Resilience program of Germany's Sovereign Tech Agency.

← git config am.threeWay

Single-Click Code Execution Exploit for Evince, Atril, and Xreader →

Michael Catanzaro's Blog

On Fedora Workstation, GNOME, Epiphany, and WebKitGTK

Log in