Sicherheitslücke in Flatpak behoben

Kürzlich wurde eine Sicherheitslücke in Flatpak entdeckt, die es bösartigen oder kompromittierten Flatpak-Anwendungen erlaubt, aus der Sandbox auszubrechen und beliebigen Code auszuführen. Die Lücke wurde als CVE-2024-32462 katalogisiert.

Die Lücke nutzt eine Schwäche im Paket xdg-desktop-portal aus, die dort mit v1.18.4 behoben wurde. Der Fehler liegt in der missbräuchlichen Verwendung der Parameter –command und –bind im Kontext des Befehls flatpak run. Diese Parameter können missbräuchlich dazu genutzt werden, zusätzliche Befehle außerhalb der Sandbox auszuführen.

Anwender des stabilen Zweigs von Flatpak müssen mindestens auf flatpak 1.14.6 aktualisieren, um auf der sicheren Seite zu sein. Für ältere Zweige sind die Versionen 1.12.9 und 1.10.9 gepatched worden, für den Entwicklungszweig wird v1.15.8 empfohlen.