KeepassXC Browser Plugin

Nach Haus telefonieren

Onkobu Tanaake

2021-05-10T10:00:00

Als ich die offenen Verbindungen an einer Desktop-Maschine durchmusterte, stieß ich auf ein paar offene Verbindungen, die keinem offenen Fenster zuzuordnen waren. Sie hatten ihren Ursprung im KeepassXC Browser-Plugin. Mit `lsof -i tcp` geht das sehr schnell.

Der Ziel-Port war immer 443, reguläre TLS-Verbindungen. Das Zitat von der Produktseite[2]:

> KeePassXC needs network access for downloading […] favicons for password entries and for providing KeePassHTTP-compatible browser extensions with access to your database.

Dort wird auch auf die Möglichkeit hingewiesen, es komplett abzustellen. Das geht bis zum Schalter für den Compiler. Auf Gentoo heißt so ein Schalter USE-Variable. Im konkreten Fall kann KeepassXC mit USE=-network installiert werden. Für mich genügte es, das Browser-Plugin zu deinstallieren und in der Konfiguration von KeepassXC den ausgehenden Verkehr abzustellen. Verbindungen weg.

Warnung

Ich habe die Inhalte nicht weiter untersucht und die Verbindungsaufnahme ist in der Dokumentation klar herausgestellt. Sie lässt sich mit einfachen Mitteln aus der Anwendung heraus unterbinden. Da ich das Browser-Plugin auf Gentoo nie zum Zugriff auf KeepassXC autorisierte – die Anwendung fragt explizit nach – wurden wohl nie Daten exfiltriert. Weniger Verbindungen bedeutet aber auch weniger Gefahrenpotenzial.

Aktualisierung 2021-06-07T21:00:00

Veröffentlichungsdatum korrigiert, war nicht in 2018.