In response to "Quick Security Evaluation - ngid-perspectives"

Joop Ringelberg 30-07-20 Version: 1

Introduction

Radically Open Security has performed a basic quick security evaluation of the Alpha InPlace program produced by the Perspectives project. Their report contains a number of recommendations. In this text I outline the course of action I intend to take with respect to these recommendations.

Electron / sandboxing issues

Running Electron-based programs distributed as an AppImage file runs into problems with sandboxing on some Linux distributions (Debian and Devuan belong to that group). Electron by default allows code in the so-called renderer process (executed by Chromium) to run un-sandboxed. However, Perspectives does not really need that. We will change the architecture in such a way that the code that runs in the renderer can run under sandbox restrictions (opening a sandboxed window).

While we are not sure this will solve the AppImage-Sandbox problem, at least this change will mitigate risks associated with Electron. Even though Perspectives does not allow navigating to arbitrary URLs (and thus loading arbitrary code!), running the renderer in sandboxed mode adds substantial security.

AppImage

Currently we build distributions using electron-builder. This tool lists a number of alternatives for AppImage for Linux distribution: snap, debian package (deb), rpm, freebsd, pacman, p5p, apk. I will look into these alternatives. It seems likely we will support at least one major package system (deb, rpm); we may follow the recommendation and drop AppImage.

Couchdb

Including CouchDB in the distribution will contribute to a better user installation experience. When InPlace moves from Alpha to a version that hopefully will have wider application, we will include CouchDB. Currently the installers are mainly used by our own team and a small group of involved parties.

Drag and drop

Drag and drop is essential to the user experience we envision for InPlace. However, the particular problem experienced by the pentester relates to dragging a file out of the InPlace window onto the desktop (or other applications). Support for this functionality in Electron seems rickety to say the least. We will drop it in favour of a file-download approach. It should be noted that this is functionality that lies somewhat outside the main InPlace areas of application (it is only for first contact between two users that cannot be connected by another, intermediary user).

Drag and drop *within* the InPlace application does not suffer from the same problem that dragging out a file does.

Distributing invitation files

We will modify the instructions/advice on how to exchange invitation json files to encourage end users to use safe(r) channels.