



redhat



ENDLESS

The Future of Linux Application Distribution

OSTree, Flatpak & GNOME Software

Richard Hughes <rhughes@redhat.com>

Mario Sánchez Prada <mario@endlessm.com>

Samsung Research UK. Staines, 2017 March 16th

About Mario

- Computer Science Engineer by the *University of Coruña*
- Open Source developer, *GNOME* Foundation member
- Previously worked at *Igalia* and *Samsung Research UK*
- Currently at *Endless Computers*, working in the *Desktop* team focused on the development of the core platform
- Your neighbour in Staines-upon-Thames since 2013

OSTree

What is OSTree?

- Git-like system for complete & bootable filesystems
- Disk efficient: de-duplication via SHA256SUM hashes, check outs files from the object store via hard links
- Network efficient: static deltas, summary file
- Reliable updates & rollback: atomicity, no inconsistencies
- Safe: GPG verification for commits and summary file
- Introspectable library and command line tools

Multiple use cases: OS deployment, efficient OTA updates, continuous integration & QA, bundled applications...

<https://ostree.readthedocs.io>

Atomic & incremental upgrades

- Git-like fetching via HTTP: simple setup
- Incremental downloads of objects, using pre-generated static deltas when available
- Automatic verification of fetched objects and deltas
- Automatic creation of new deployments (+ 3-way merge)
- Atomic swapping of boot configurations via symlinks

```
$ ls -l /ostree/
total 12K
lrwxrwxrwx 1 root root    8 Oct  4 16:55 boot.0 -> boot.0.1
drwxr-xr-x 3 root root 4.0K Oct  4 16:55 boot.0.1
drwxr-xr-x 3 root root 4.0K Oct  4 16:55 deploy
drwxr-xr-x 7 root root 4.0K Mar 12 12:59 repo
```

Some internal details

Anatomy of an OSTree repository:

- Types of repositories: bare, bare-user, archive-z2
- Objects (commits, dirtree, dirmeta, content) + refs
- The summary file

OSTree deployments:

- Multiple deployments per OS, parallel installable
- Shared stateful data among deployments (/etc, /var)

Comparison with other systems

OSTree vs APT/RPM

- Deploying full filesystem VS partial ones
- Truly atomic VS potentially broken intermediate stages
- No dependencies hell, no postinst/postrm hooks...

OSTree vs image replication (flashing)

- Predictable like flashing, but much more efficient
- Only 2 persistent directories supported: /etc & /var
- Works on top of any filesystems supporting hard links
- Supports installing different versions of the OS in parallel

Who is using OSTree?

- Atomic project (Fedora, CentOS)
- GNOME Continuous
- Qt OTA updates
- Automotive Grade Linux (AGL)
- Endless OS
- Flatpak

Flatpak

What is Flatpak?

- A new way of distributing applications in Linux
- Sits on top of OSTree and *bubblewrap* (chroot on steroids)
- Cross-platform by design: **runtimes** and **applications**
- Reliable and secure: GPG signatures, sandboxing, portals...
- Allows having both user and system-wide installations
- Open Source project. Started by Red Hat, contributions from Endless, Collabora, Codethink, Intel, Kinvolk, Solus...

Similar in some ways to Docker, but with the focus on end user applications instead of for containerized system-wide services.

<http://flatpak.org>

A brief note on bubblewrap

- Allows running sandboxed applications in chroot-like environments as an **unprivileged user**
- Creates a mount namespace with / on a tmpfs
- Uses PR_SET_NO_NEW_PRIVS when cloning the process to limit what the binary can do after dropping privileges
- Implements a subset of the Kernel's user namespaces feature to isolate processes
- More namespaces: CLONE_NEWUSER, CLONE_NEWIPC, CLONE_NEWPID, CLONE_NEWNET, CLONE_NEWUTS
- Allows passing a list of *seccomp* filters to limit *syscalls*

Bubblewrap example

```
[fedoravm ~]$ bwrap --ro-bind /usr /usr --ro-bind /etc/resolv.conf /etc/resolv.conf \
--symlink usr/lib /lib --symlink usr/lib64 /lib64 --symlink usr/bin /bin \
--dir /tmp --proc /proc --dev /dev \
--unshare-pid --unshare-net \
--chdir / \
/bin/sh

sh-4.3$ ls /
bin dev etc lib lib64 proc tmp usr

sh-4.3$ ls /dev/
console full null ptmx pts random shm stderr stdin stdout tty urandom zero

sh-4.3$ ls -l /etc/
total 4
-rw-r--r-- 1 65534 65534 53 Mar 14 00:46 resolv.conf

sh-4.3$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1 (Local Loopback)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

sh-4.3$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME COMMAND
1000          1  0.0  0.0 15472   160 ?        S    01:28  0:00 bwrap --ro-bind /usr /usr --
1000          2  0.0  0.1 122136  3608 ?        S    01:28  0:00 /bin/sh
1000          8  0.0  0.1 150020  3544 ?        R+   01:29  0:00 ps aux
```

Anatomy of a Flatpak Runtime

```
$ tree -L 3 /var/lib/flatpak/runtime/org.gnome.Platform/x86_64/3.22/active/
|-- deploy
|-- files
|   |-- bin
|   |   |-- [...]
|   |   |-- basename
|   |   |-- bash
|   |   |   |-- [...]
|   |   |-- etc
|   |   |   |-- [...]
|   |   |-- ca-certificates.conf
|   |   |-- dbus-1
|   |   |   |-- [...]
|   |   |-- lib
|   |   |   |-- [...]
|   |   |-- libglib-2.0.so.0.5000.2
|   |   |-- libGL.so -> libGL.so.1.0.0
|   |   |   |-- [...]
|   |-- lib64
|   |   '-- ld-linux-x86-64.so.2 -> /usr/lib/ld-linux-x86-64.so.2
|   |-- [...]
|   |-- manifest-base-1.json
|   |-- manifest.json
|   |-- sbin -> bin
|   |-- share
|   |   |-- [...]
|   |   |-- applications
|   |   |   |-- [...]
|   '-- var
|       |-- cache
|       |-- lib
|           '-- run
`-- metadata
```

Anatomy of a Flatpak Application

```
$ tree -L 3 /var/lib/flatpak/app/org.gnome.Todo/current/active/
/var/lib/flatpak/app/org.gnome.Todo/current/active/
|-- deploy
|-- export
|   '-- share
|       |-- applications
|       |-- dbus-1
|       '-- icons
|-- files
|   |-- bin
|   |   '-- gnome-todo
|   |-- lib
|   |   |-- debug
|   |   |-- evolution-data-server
|   |   |-- girepository-1.0
|   |   |-- gnome-todo
|   |   |-- goa-1.0
|   |   |-- libcamel-1.2.so -> libcamel-1.2.so.59.0.0
|   |   |-- [...]
|   |   '-- systemd
|   '-- manifest.json
`-- share
    |-- appdata
    |-- applications
    |-- dbus-1
    |-- GConf
    |-- gir-1.0
    |-- glib-2.0
    |-- icons
    |-- locale
    |-- pixmaps
    '-- runtime
`-- metadata
```

Putting all together: inside a running flatpak app

```
./flatpak-info
/app
  /app/bin
  /app/lib
  /app/share
  [...]
/bin
/dev
  /dev/console
  /dev/full
  /dev/null
  [...]
/etc
[...]
/home/mario
  /home/mario/.config
  /home/mario/.local/share/flatpak
  /home/mario/.var/app/org.gnome.Todo
/lib
/lib64
/local
/proc
  /proc/1
  /proc/1/attr
  [...]
/run
  /run/build
  /run/build-runtime
  /run/host
  /run/systemd
  /run/user/1000
  [...]
[...]
/run/user/1000
  /run/user/1000/Xauthority
  /run/user/1000/app
  /run/user/1000/app/org.gnome.Todo
  /run/user/1000/bus
  /run/user/1000/dconf
  /run/user/1000/dconf/user
  /run/user/1000/doc
  /run/user/1000/flatpak-info
  [...]
/sbin
/sys
  /sys/block
  [...]
/tmp
  /tmp/.X11-unix
  /tmp/.X11-unix/X99
  [...]
/usr
  /usr/bin
  /usr/share
  /usr/share/applications
  [...]
/var
  /var/cache
  /var/config
  /var/config/user-dirs.dirs
  [...]
  /var/data
  /var/run
  /var/tmp
```

Platform and SDK Runtimes

Two types of runtimes:

- Platform runtime: just the bits needed to **run** apps
- SDK runtime: platform + the necessary tools and files for development purposes (e.g. headers, debug symbols...)

Currently **two main standard runtimes** available:

- Freedesktop runtime: contains a set of essential libraries and services: D-Bus, GLib, PulseAudio, X11, Wayland
- GNOME runtime: based on the Freedesktop runtime, adds libraries like GTK+, GStreamer or GVFS on top.

A KDE runtime is currently under development too:
<https://github.com/KDE/flatpak-kde-runtime>

The Sandbox

Limited access to the host system by default:

- No access to processes outside the sandbox (*namespaces*)
- No access to the network, session bus and devices
- Controlled execution of certain *syscalls* (*seccomp* filters)
- Read-only access to the runtime and app (*bind mounts*)
- Read-write access to \$HOME/.var/app/\$APPID
- Controlled access to resources (*cgroups*)
- No access to host services (e.g. X/Wayland, system bus...)

Flatpak's sandbox is very limiting by default, but there are ways of dealing with that to run real-word applications...

Escaping the Sandbox: fine-grained permissions

Easiest way to work with the sandbox is to open “holes” in it:

- Grant access to UNIX domain sockets: X.org, Wayland, PulseAudio, System and Session D-Bus...
- Grant access to specific devices: dri, kvm
- Grant access to see, use and/or own specific D-Bus names
- Share specific subsystems with the host (network, IPC)
- Fine-grained permissions for filesystem access
- Define extensions for runtimes or applications (e.g. 110n)

Combining all this enables makes it possible to run apps in a more controlled way, but it's not very secure.

The manifest file

A Flatpak manifest file (metadata):

```
[Application]
name=org.gnome.Calculator
runtime=org.gnome.Platform/x86_64/3.20
sdk=org.gnome.Sdk/x86_64/3.20
command=gnome-calculator

[Context]
shared=network;ipc;
sockets=x11;wayland;
filesystems=xdg-run/dconf;~/.config/dconf:ro;

[Session Bus Policy]
ca.desrt.dconf=talk

[Environment]
DCONF_USER_CONFIG_DIR=.config/dconf

[Extension org.gnome.Calculator.Locale]
directory=share/runtime/locale
subdirectories=true

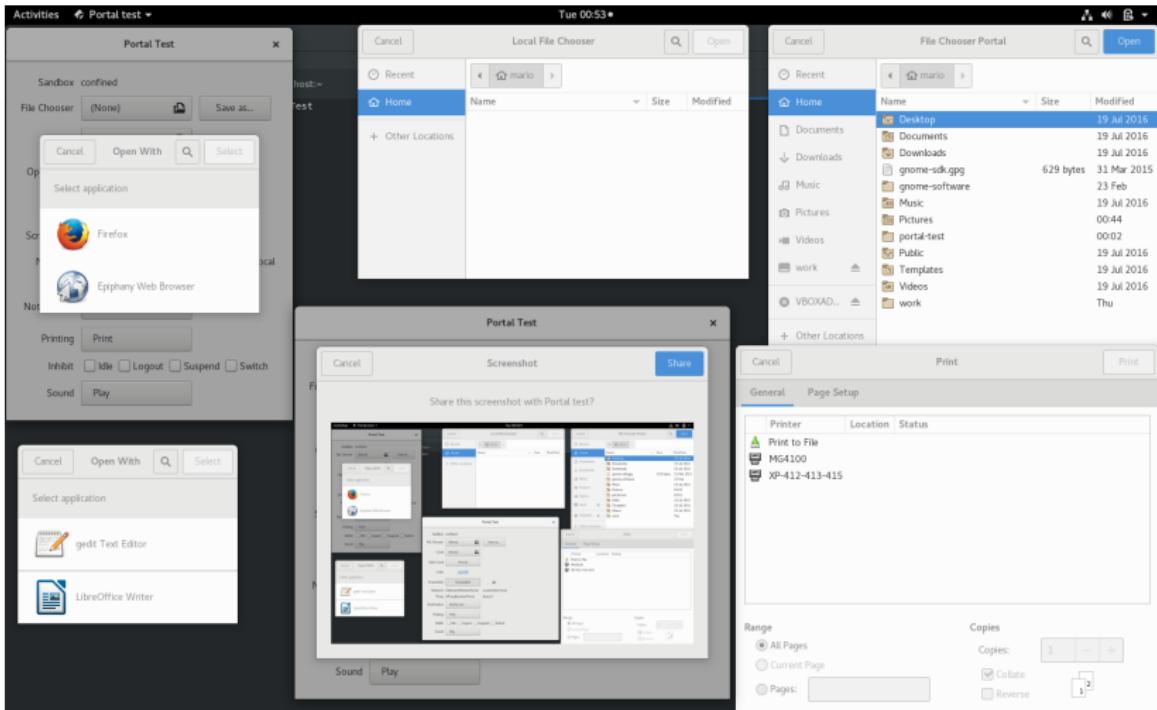
[Extension org.gnome.Calculator.Debug]
directory=lib/debug
```

Escaping the sandbox: Portals

- High-level APIs to allow sandboxed apps request access
- Out-of-process services running on the host system
- Sandboxed apps communicate via D-Bus
- Different types of portals for different needs:
 - NetworkMonitor, OpenURI, Filechooser, Documents, Printing, Geolocation, Screenshots, Notifications, Proxy...
- Using portals is **safe**:
 - They don't expose sensitive information from the host
 - Portal-initiated operations are **interactive** and **cancellable**
- Split in UI-less frontend + desktop-specific backends:
 - Currently backends for GTK+, with KDE work-in-progress.
 - GLib & GTK+ include support for several portals since 3.22

Flatpak Portals: GTK+ backends

```
$ flatpak run org.gnome.PortalTest
```



Building a flatpak apps

```
{  
    "id" : "org.gnome.Todo",  
    "branch" : "stable",  
    "runtime" : "org.gnome.Platform",  
    "runtime-version" : "3.22",  
    "sdk" : "org.gnome.Sdk",  
    "build-options" : {  
        "cflags" : "-O2 -g",  
        "cxxflags" : "-O2 -g",  
        "env" : {  
            "V" : "1"  
        }  
    },  
    "command" : "gnome-todo",  
    "modules" : [  
        {  
            "name" : "gnome-online-accounts",  
            "config-opts" : [  
                "--disable-telepathy",  
                "--disable-documentation",  
                "--disable-backend"  
            ],  
            "sources" : [  
                {  
                    "url" : "https://download.gnome.org/sources/gnome-online-accounts/3.22/gnome-online-accounts-3.22.0.tar.xz",  
                    "sha256" : "aacce93a71bf5e687a45ae0d00f31ea0625ddd8143235d6d8c64c4ec21bbfa33",  
                    "type" : "archive"  
                }  
            ]  
        },  
        [...] ---> More dependencies here  
    ]  
}
```

Building a flatpak apps (II)

```
[...]
{
  "name" : "gnome-todo",
  "sources" : [
    {
      "url" : "https://download.gnome.org/sources/gnome-todo/3.22/gnome-todo-3.22.1.tar.xz",
      "sha256" : "cb80f64f5edeeac7b221146d2203bd1bebc49d275b7a41e7a5418f409d9c74af",
      "type" : "archive"
    }
  ]
},
"cleanup" : [
  "/include", "/lib/pkgconfig", "/share/pkgconfig", "/share/aclocal", "/man",
  "/share/man", "/share/gtk-doc", "/share/vala", "*.*.la", "*.*.a"
],
"finish-args" : [
  "--share=ipc",
  "--socket=x11",
  "--socket=wayland",
  "--share=network",
  "--talk-name=org.gnome.OnlineAccounts",
  "--talk-name=org.gnome.evolution.dataserver.AddressBook9",
  "--talk-name=org.gnome.evolution.dataserver.Calendar7",
  "--talk-name=org.gnome.evolution.dataserver.Sources5",
  "--talk-name=org.gnome.evolution.dataserver.Subprocess.Backend.*",
  "--filesystem=xdg-run/dconf",
  "--filesystem=~/config/dconf:ro",
  "--talk-name=ca.desrt.dconf",
  "--env=DCONF_USER_CONFIG_DIR=.config/dconf"
]
}
```

Application distribution

- Publish your local repository: `build-export`
 - Export your app to an OSTree (archive-z2) repository
 - You could publish this repository now over HTTP
- Sign everything: `build-sign`, `build-update-repo`
 - Important to GPG-sign the commits and the summary file
 - Allows using unencrypted HTTP (faster downloads)
 - Recommended to create a dedicated GPG key
- Push to a production public repository: e.g. `rsync`
 - Simple requirements: static files served over HTTP!
 - Push it to your public server once you're happy
 - Order your commands wisely (avoid race conditions)

Application distribution (II)

- Configure your public repository appropriately:
 - `build-update-repo -title=<title>`
 - `build-update-repo -default-branch=<branch>`
- Provide efficient updates:
 - Enable HTTP keep-alive in the server (lots of files)
 - Use OSTree's static-deltas feature (good for big files)
 - Run `build-update-repo` everytime an app changes
- Generate application metadata for software centers:
 - Generate AppStream data for each application in your repo:
`build-update-repo` will put it an `appstream` branch
 - Make sure your apps must export an AppData XML file!

Flatpak filetypes: .flatpakrepo and .flatpakref

Configuring flatpak “repositories”: gnome.flatpakrepo

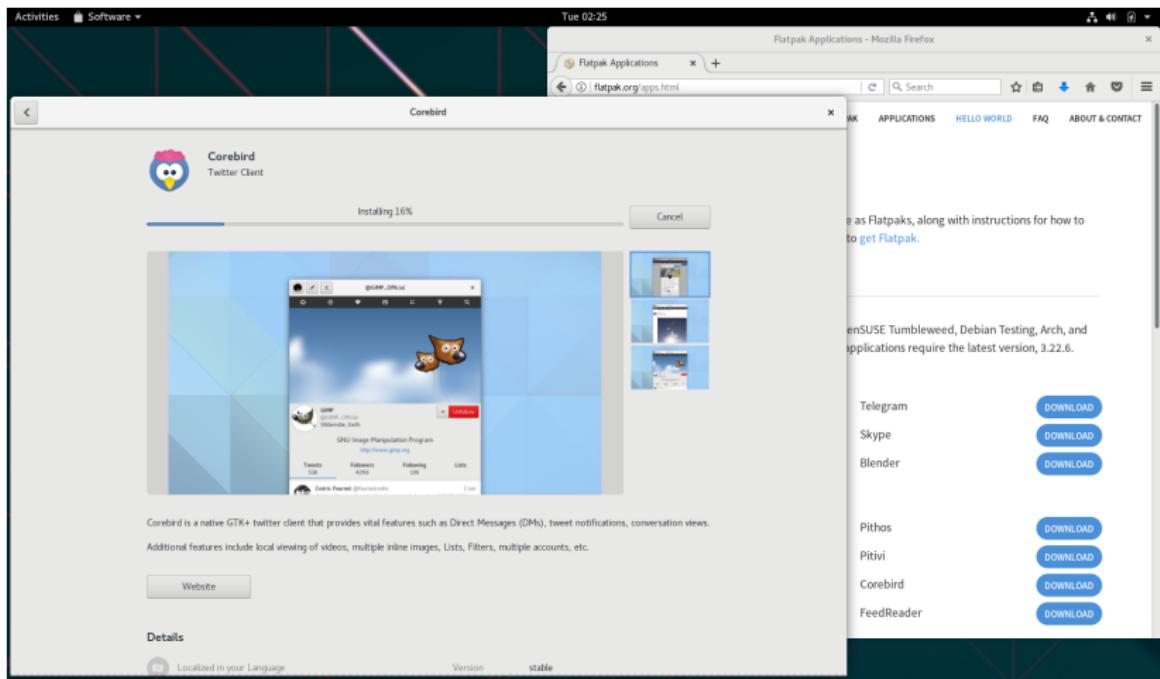
```
[Flatpak Repo]
Title=Gnome Stable Runtimes
Url=http://sdk.gnome.org/repo/
Homepage=https://www.gnome.org/get-involved/
Comment=The standard Gnome runtime used by most gnome apps
Description=GNOME runtimes are released with each major release and contain the main GNOME platform libraries. At the moment they only receive minor bug fixing and security updates, but should be considered ABI stable and frozen.
Icon=https://www.gnome.org/wp-content/themes/gnome-grass/images/gnome-logo.png
GPGKey=mQENBFUU[...]15w8jmY=
```

Installing an application: gnome-recipes.flatpakref

```
[Flatpak Ref]
Title=GNOME Recipes
Name=org.gnome.Recipes
Branch=master
Url=https://matthiasclasen.github.io/recipes-releases/repo
IsRuntime=False
GPGKey=mQENBFis[...]Kpp5G2YW
RuntimeRepo=https://sdk.gnome.org/gnome.flatpakrepo
Comment=GNOME loves to cook
```

Installing a flatpak application in one click

GNOME Software, flatpak and .flatpakref files in action:



References:

- » *OSTree documentation*: <https://ostree.readthedocs.io/en/latest>
- » *Project Atomic*: <https://www.projectatomic.io>
- » *GNOME Continuous*: <https://wiki.gnome.org/Projects/GnomeContinuous>
- » *Qt OTA updates*: <https://doc.qt.io/QtOTA>
- » *Automotive Linux*: <https://automotivelinux.org>
- » *Endless OS*: <https://endlessos.com>
- » *Bubblewrap*: <https://github.com/projectatomic/bubblewrap>
- » *Flatpak documentation*: <https://docs.flatpak.org/en/latest>
- » *Flatpak portals*: <https://github.com/flatpak/xdg-desktop-portal>
- » *Flatpak portals (GTK)*: <https://github.com/flatpak/xdg-desktop-portal-gtk>
- » *Alex Larsson's blog*: <https://blogs.gnome.org/alexl>
- » *Christian Hergert's talk on Scale15x*: <https://hergert.me/talks/Flatpak-Scale-15x.pdf>



GNOME Software

Add/Remove Software

System Filters Selection Help

Find

- All packages
- Package collections
- Admin tools
- GNOME desktop
- KDE desktop
- Other desktops
- XFCE desktop
- Education
- Fonts
- Games
- Graphics
- Internet
- Legacy
- Localisation

-  Simple menu editor for GNOME
alacarte-0.11.5-1.fc9 (noarch)
-  Assistive Technology Service Provider Interface
at-spi-1.22.1-1.fc9 (i386)
-  Bluetooth pairing and control applet
bluez-gnome-0.26-1.fc9 (i386)
-  A bug reporting utility for GNOME
bug-buddy-1:2.22.0-2.fc9 (i386)
-  A desktop recorder
byzanz-0.1.1-6.fc9 (i386)
-  Compiz gnome integration bits
compiz-gnome-0.7.6-3.fc9.1 (i386)

Alacarte is a menu editor for GNOME that lets you get things done, simply and quickly. Just click and type to edit, add, and delete any menu entry.

Project: [Homepage](#)
Group: GNOME desktop
License: GPLv2+
Installed size: 462.4 KB

Help

 Clear

 Apply



Local file conflict between packages



Two packages provide the same file.
This is usually due to mixing
packages from different software
sources.

▷ **More details**

Close

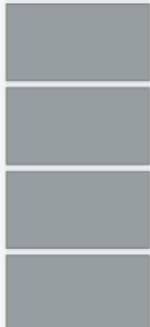
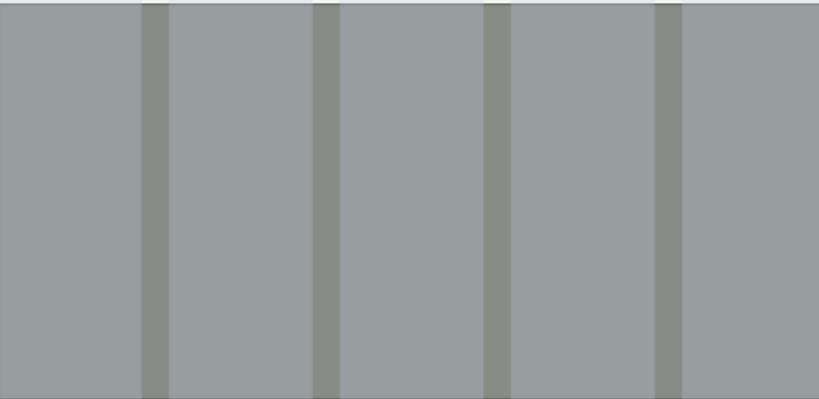
co-op'er-a-tion or **co-o-**
tio]] 1 the act of coope-
ciation of a number of
or profits 3 *Ecol.* an in-
beneficial to all those

Blender

Blender
3D modeling, animation, rendering and post production.

Install

★★★★★ (22)



Blender provides a broad spectrum of modeling, texturing, lighting, animation and video post-processing functionality in one package. Through its open architecture, Blender provides cross-platform interoperability, extensibility, an incredibly small footprint, and a tightly integrated workflow. Blender is one of the most popular Open Source 3D graphics applications in the world.

Aimed at media professionals and artists world-wide, Blender can be used to create 3D visualizations and still images, as well as broadcast- and cinema-quality videos, while the incorporation of a real-time 3D engine allows for the creation of 3D interactive content for stand-alone playback.

[Read more...](#)

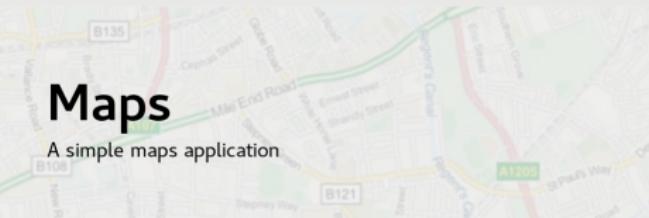
[All](#)[Installed](#)[Updates](#)

4



Maps

A simple maps application



Categories

 [Audio & Video](#) [Communication & News](#) [Games](#) [Graphics & Photography](#) [Productivity](#) [Add-ons](#)

Editor's Picks



```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2013 Richard Hughes &lt;richard@hughsie.com&gt; --&gt;
&lt;component type="desktop"&gt;
  &lt;id&gt;org.gnome.Software.desktop&lt;/id&gt;
  &lt;metadata_license&gt;CC0-1.0&lt;/metadata_license&gt;
  &lt;project_license&gt;GPL-2.0+&lt;/project_license&gt;
  &lt;_name&gt;GNOME Software&lt;/_name&gt;
  &lt;_summary&gt;Application manager for GNOME&lt;/_summary&gt;
  &lt;description&gt;
    &lt;p&gt;
      Software allows you to find and install new applications
      extensions and remove existing installed applications.
    &lt;/p&gt;
  &lt;/description&gt;
&lt;/component&gt;</pre>
```

[All](#)[Installed](#)[Updates](#)

8

 polar **Polaris**

A simple Internet Relay Chat (IRC) client that is designed to integrate seamlessly with GNOME; it features a simple and beautiful interface which allows you to focus on your c...
Source: fedoraproject.org

**Polaris**

A simple Internet Relay Chat (IRC) client that is designed to integrate seamlessly with GNOME; it features a simple and beautiful interface which allows you to focus on your c...
Source: sdk.gnome.org

Installed

GNOME Software Plugin API

Table of Contents

[**GsAppList**](#) — An application list

[**GsApp**](#) — An application that is either installed or that can be installed

[**GsAuth**](#) — User data used for authentication

[**GsOsRelease**](#) — Data from os-release

[**GsPlugin Helpers**](#) — Runtime-loaded modules providing functionality

[**GsPlugin Exports**](#) — Vfuncs that plugins can implement

[**GsReview**](#) — An application user review

[**GsUtils**](#) — Utilities that plugins can use

★★★★★ It just works...

22 April 2016

usr01

Hands down, the easiest to use and most reliable scanner software I've encountered - on any platform.

Was this review useful to you? Yes | No

Report...

★★★★★ Works great with my CanoScan

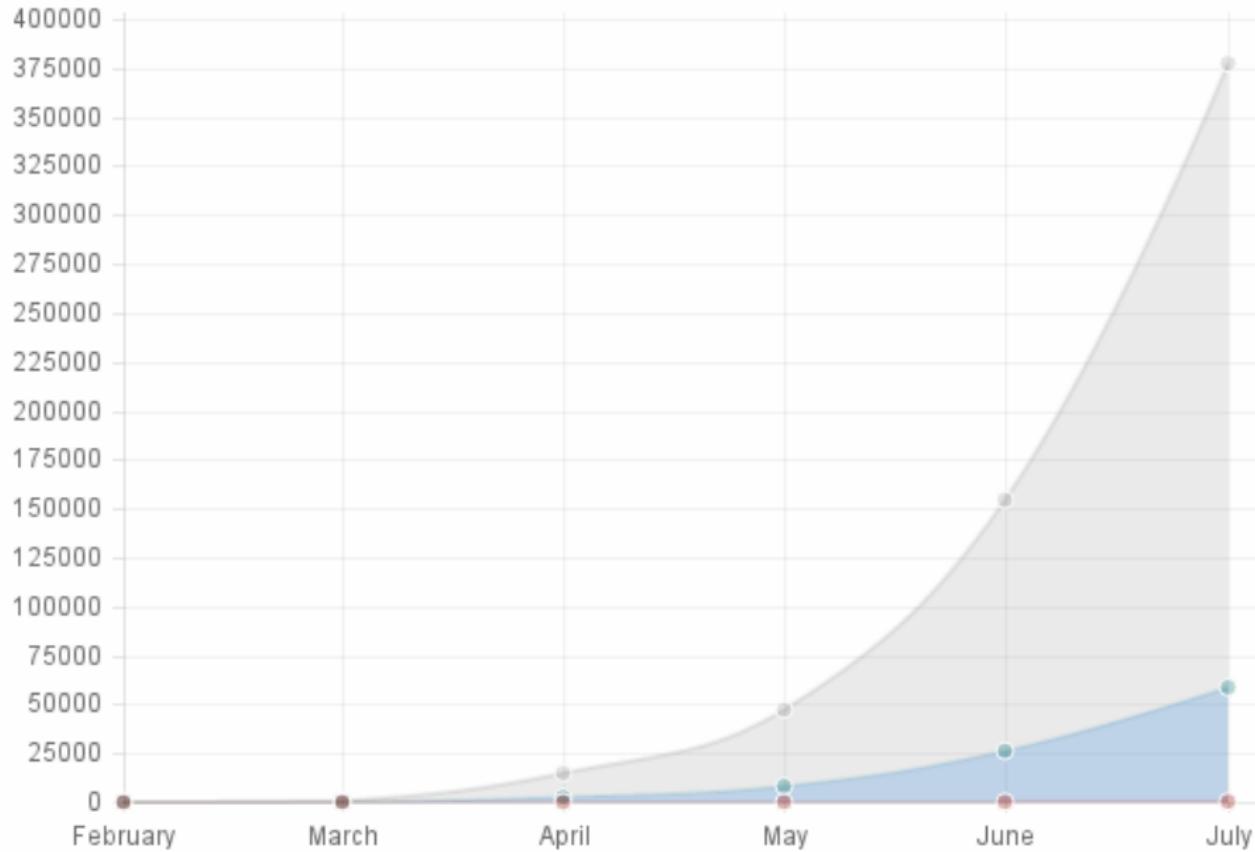
10 February 2016

Richard Hughes

This is easy to use and works really well with my scanner. The saved PDF file is clear and easy to read.

Was this review useful to you? Yes | No

Report...



Phoenix - Award Workstation BIOS CMOS Setup Utility

- ▶ Standard CMOS Features
- ▶ Advanced BIOS Features
- ▶ Advanced Chipset Features
- ▶ Integrated Peripherals
- ▶ Power Management Setup
- ▶ PnP/PCI Configurations
- ▶ PC Health Status
- ▶ Frequency/Voltage Control
- ▶ Load Performance Defaults
- ▶ Load Optimized Defaults
- ▶ Set Supervisor Password
- ▶ Set User Password
- ▶ Save & Exit Setup
- ▶ Exit Without Saving

Esc : Quit

↑ ↓ ← → : Select Item

F10 : Save & Exit Setup

Time, Date, Hard Disk Type...



LibreOffice

LibreOffice is a powerful office suite. Its clean interface and feature-rich tools help you unleash your creativity and enh...

Update



Freedesktop.org Application Platform version 1.4

Shared libraries provided by freedesktop.org

Update



GNOME Application Platform version 3.22

Shared libraries used by GNOME applications

Update



GNOME Software Development Kit version master (Nightly)

Tools and headers for developing applications using the GNOME application platform

Update

Device Firmware



ColorHugALS 3.0.2 ▶ 4.0.3

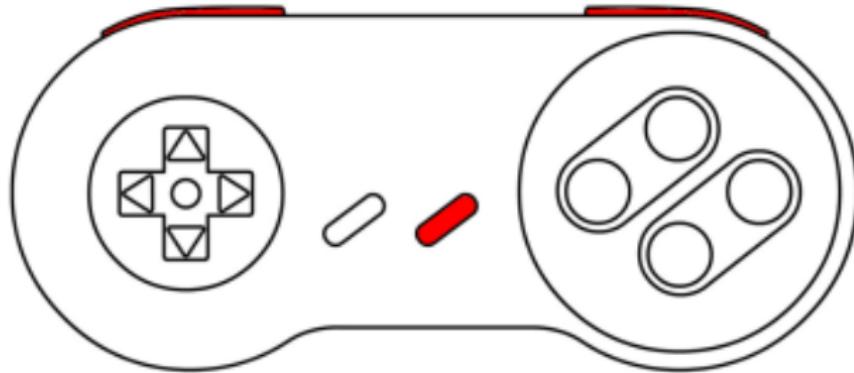
Version 4.0.3: Remove the invalid .inf file from the release tarball. No code or behaviour changes. Version 4.0.2: We n...

Update

Device cannot be used during update.

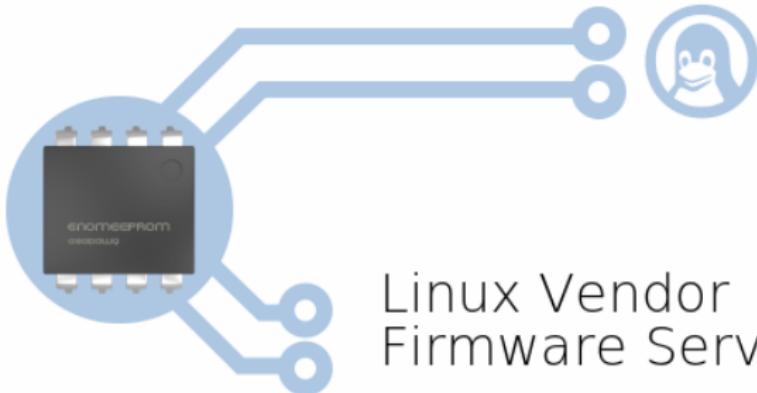
Prepare 8Bitdo SFC30

Unplug the controller, hold down L+R+START for 3 seconds until both LEDs are flashing then reconnect the controller.



Cancel

Install



Linux Vendor Firmware Service

Please Login

The Linux Vendor Firmware Service is a secure portal which allows hardware vendors to upload firmware updates. Files can be uploaded privately and optionally embargoed until a specific date.

This site is used by all major Linux distributions to provide metadata for clients such as fwupd and GNOME Software. To upload firmware please login, or [request a new account](#).

Username:

Password:

All

Installed

Updates

Fedora 24 Ready to be Installed

A major upgrade, with new features and added polish.

It is recommended that you back up your data and files before upgrading.



Replace Installed Version of Blender?

A version of Blender is already installed. You can choose to replace the existing version, or install the new version alongside.

Installed Version



Blender

Version 2.76-2.23

Source <distribution>



New Version



Blender

Version 2.76

Source Blender Foundation



Cancel

Parallel Install

Replace

A.O..

"TEASEF

TLW

QUESTION
EVERYTHING

Thank you!