

Firmware updates for pfSense and OPNsense with fwupd/LVFS

FOSDEM22

Norbert Kamiński



- Project genesis
- Overall information about fwupd
- fwupd tool architecture
- pfSense proof of concept
- OPNSense proof of concept
- Existing issues and future steps
- Q&A

Many thanks to my colleague - Michał Kopeć, who did OPNsense proof of concept work.



Norbert Kamiński
Embedded Systems Engineer

- open-source contributor:
 - fwupd
 - meta-pcengines
- scope of interests:
 - firmware upgrade tools
 - virtualization
 - embedded Linux
-  norbert.kaminski@3mdeb.com
-  [linkedin.com/in/norbert-kami%C5%84ski/](https://www.linkedin.com/in/norbert-kami%C5%84ski/)
-  [facebook.com/nkaminski3](https://www.facebook.com/nkaminski3)
-  [@_asiderr](https://twitter.com/_asiderr)



- coreboot licensed service providers since 2016 and leadership participants
- UEFI Adopters since 2018
- Yocto Participants and Embedded Linux experts since 2019
- Official consultants for Linux Foundation fwupd/LVFS project since 2020
- IBM OpenPOWER Foundation members since 2020

- Routers always were important target for various adversaries, therefore they must be appropriately protected
- It is almost impossible to update device firmware without proper tools
- Our products - [Basic firmware update integration](#) and open-source firmware [Dasharo](#) will benefit from this integration



DASHARO

- fwupd project can query supported hardware for the current firmware versions and also deploy new firmware versions to devices
- LVFS is a secure web service that provides information about available firmware updates. It can be used by the OEM's to upload firmware archives downloaded by the users
- fwupd could be a good way to simplify the deployment of firmware updates for firewall device and to facilitate the update process for end-users



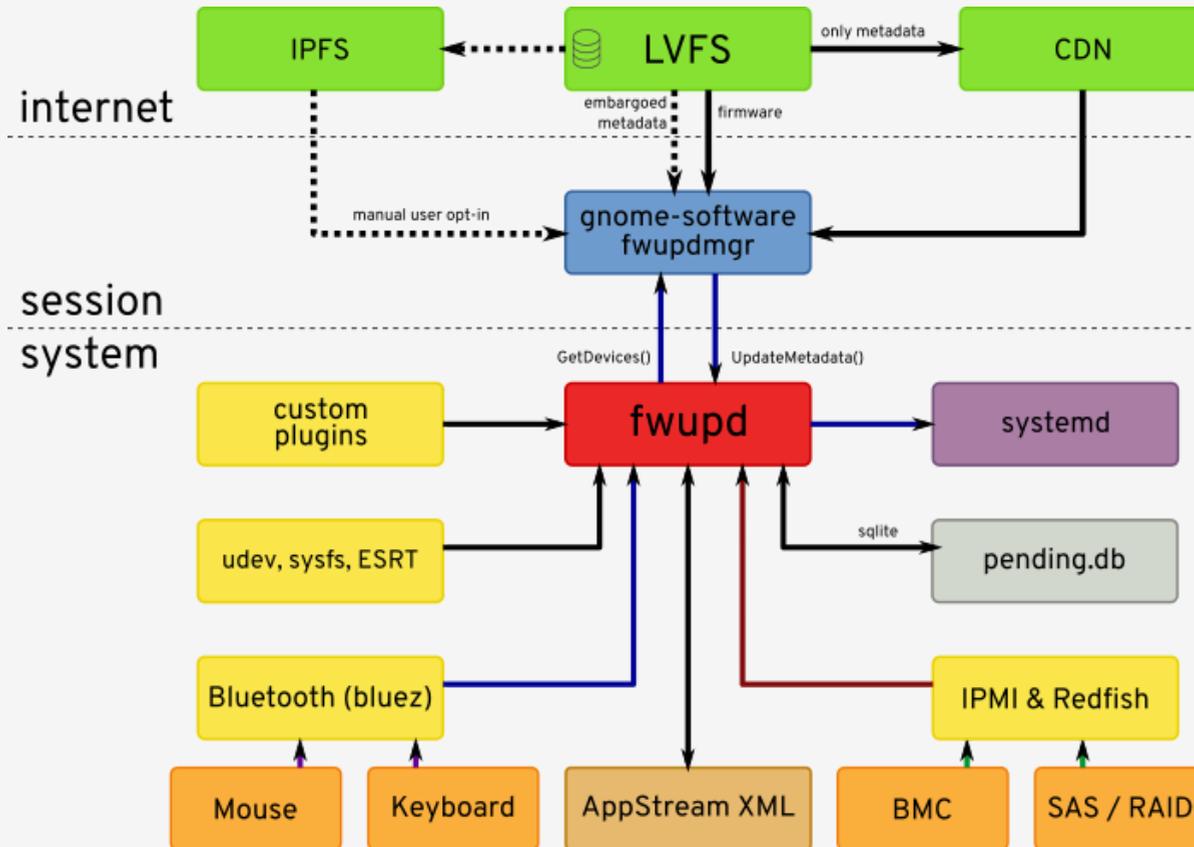


Image source: <https://lvfs.readthedocs.io/en/latest/intro.html>



- The LVFS is a secure web service that is used by OEM's to provide firmware updates
- The LVFS provides metadata that contains information about possible updates
- The firmware updates are packed into cabinet archives. The archive contains the firmware blob, information about the update, and jcat file, which is used to verify the firmware updates
- A manufacturer is signing the firmware and this sign is verified during the update



pfSense is a free and open-source firewall and router that also features unified threat management, load balancing, multi-WAN, and more. It is based on FreeBSD.

Hardware and software stack:

- PC Engines apu2 - Router/firewall board
- pfSense 2.5.2
- fwupd 1.7.4
- FreeBSD 12.2 VM

- The first step was the installation of the pfSense 2.5.2 at apu2
- The next step was the enablement of the FreeBSD pkg repo in the pfSense

```
vi /usr/local/etc/pkg/repos/pfSense.conf
```

```
FreeBSD: {  
  url: "pkg+<http://pkg.freebsd.org/FreeBSD:12:amd64/release_2>",  
  signature_type: "fingerprints",  
  fingerprints: "/usr/share/keys/pkg",  
  mirror_type: "srv",  
  enabled: yes  
}
```

- As it is mentioned in the [documentation](#), the packages for pfSense should be compiled in the FreeBSD VM

- We used FreeBSD 12.2 virtual machine to create fwupd package for pfSense 2.5.2
- We created the fwupd package and its dependencies in [3mdeb's FreeBSD ports fork](#)

```
PORTNAME= fwupd
DISTVERSION= 1.7.5
GH_TAGNAME= 38bab8f
CATEGORIES= sysutils

MAINTAINER= norbert.kaminski@3mdeb.com
COMMENT= Update firmware automatically, safely, and reliably

LICENSE= LGPL21

BUILD_DEPENDS= gtkdoc-scan:textproc/gtk-doc \
  help2man:misc/help2man \
  vala:lang/vala \
  ${LOCALBASE}/libexec/fwupd/efi/fwupdx64.efi.sysutils/fwupd-efi \
  ${PYTHON_PKGNAMEPREFIX}gobject3>0:devel/py-gobject3@${PY_FLAVOR}
LIB_DEPENDS= libcurl.so:ftp/curl \
  libgcab-1.0.so:archivers/gcab \
  libgnutls.so:security/gnutls \
  [...]
USES= gnome libarchive meson pkgconfig python:3.8+ shebangfix sqlite
USE_GITHUB= yes
[...]
MESON_ARGS= -Dgudev=false \
  -Dplugin_amt=false \
  -Dplugin_dell=false \
  -Dplugin_emmc=false \
  -Dplugin_nvme=false \
  -Dplugin_parade_lscon=false \
  [...]
.include <bsd.port.mk>
```

- We installed fwupd dependencies in the FreeBSD VM and in the pfSense to comply with all of the build and runtime dependencies

```
pkg install -y git python3 glib meson pkgconf gobject-introspection \  
    vala gtk-doc json-glib gpgme gnutls sqlite3 curl gcab libarchive \  
    libgpg-error gettext-tools gtk-update-icon-cache atk pango \  
    binutils gcc protobuf-c efivar
```

- The next step was cloning our fork in the FreeBSD VM:

```
git clone <https://github.com/3mdeb/freebsd-ports.git> -b fwupd-pfsense --depth 1 /usr/ports
```

- Then we built fwupd dependencies and fwupd package that were not currently in the FreeBSD ports - devel/libgusb, textproc/libjcat, textproc/libxmlb, and sysutils/fwupd



- The created packages were sent to the pfSense via scp
- Then we installed the fwupd dependencies and fwupd itself:

```
pkg add ./libgusb-0.3.7.pkg ./libjcat-0.1.8.pkg ./libxmlb-0.3.6.pkg ./fwupd-1.7.5.pkg
```

- The last step was running dbus:

```
service dbus onestart
```

```

10:36:58:0182 FuEngine      disabling plugin because: failed to startup using msr: missing kernel support
10:36:58:0182 FuPlugin     coldplug(cpu)
10:36:58:0183 FuDevice     removing vendor prefix of 'AMD' from 'AMD GX-412C SOC'
10:36:58:0186 FuDevice     using 4bde70ba4e39b28f9eab1628f9dd6e6244c03027 for cpu:0
10:36:58:0186 FuPlugin     emit added from cpu: 4bde70ba4e39b28f9eab1628f9dd6e6244c03027
10:36:58:0227 FuPlugin     fu_plugin_device_registered(dell_dock)
10:36:58:0227 FuPlugin     fu_plugin_device_registered(uefi_pk)
10:36:58:0227 FuPlugin     fu_plugin_device_registered(usi_dock)
10:36:58:0228 FuDeviceList  ::added 4bde70ba4e39b28f9eab1628f9dd6e6244c03027
10:36:58:0228 FuPlugin     coldplug(uefi_pk)
10:36:58:0228 FuEngine     disabling plugin because: failed to coldplug using uefi_pk: failed to parse PK: invalid firmware as zero sized
10:36:58:0228 FuEngine     using plugins: analogix, ccgx, colorhug, cpu, cross_ec, dell_dock, dfu, dfu_csr, ebitdo, elanfp, fastboot, fresco_pd, goodixmoc, hailuck, jabra, logitech_bulkcontroller, nitrokey, rts54hid, rts54hub, steelseries, synaptics_cape, synaptics_cxaudio, synaptics_prometheus, system76_launch, usi_dock, vli, wacom_usb
10:36:58:0293 FuDevice     using 73ef80b60058b4f18549921520bfd94eaf18710a for usb:00:04
10:36:58:0384 FuDevice     changing verfmt for 73ef80b60058b4f18549921520bfd94eaf18710a: bcd->triplet
10:36:58:0384 FuDevice     changing version for 73ef80b60058b4f18549921520bfd94eaf18710a: 0.2->2.0.7
10:36:58:0422 FuPlugin     emit added from colorhug: 73ef80b60058b4f18549921520bfd94eaf18710a
10:36:58:0446 FuPlugin     fu_plugin_device_registered(dell_dock)
10:36:58:0446 FuPlugin     fu_plugin_device_registered(usi_dock)
10:36:58:0446 FuDeviceList  ::added 73ef80b60058b4f18549921520bfd94eaf18710a
10:36:58:0466 FuEngine     Emitting PropertyChanged('Status'='idle')
10:36:58:0466 FuMain       Emitting PropertyChanged('Status'='idle')
10:36:58:0486 FuEngine     ignoring 2.0.7 == 2.0.7
10:36:58:0486 FuEngine     ignoring 2.0.5 < 2.0.7
10:36:58:0486 FuEngine     ignoring 2.0.6 < 2.0.7
10:36:58:0486 FuEngine     ignoring 2.0.2 < 2.0.7
10:36:58:0506 FuEngine     writing motd target /var/local/cache/fwupd/motd.d/85-fwupd
10:36:58:0508 GLib-GIO    Failed to initialize portal (GMemoryMonitorPortal) for gio-memory-monitor: Not using portals
10:36:58:0512 GLib-GIO    _g_io_module_get_default: Found default implementation dbus (GMemoryMonitorDBus) for .gio-memory-monitor
10:36:58:0517 FuMain       Daemon ready for requests (locale en_GB.UTF-8)
10:36:58:0529 FuMain       acquired name: org.freedesktop.fwupd
10:37:13:0116 FuPlugin     add_security_attrs(uefi_pk)
10:37:13:0117 FuPlugin     add_security_attrs(msr)
10:37:13:0118 FuHistory    parsing 2022-01-28 10:28:45
10:37:13:0119 FuEngine     skipping writing HSI attrs to database as unchanged
10:37:13:0123 FuMain       Called SetHints()
10:37:13:0123 FuMain       got hint locale=en_GB.UTF-8
10:37:44:0584 FuMain       Called SetHints()
10:37:44:0584 FuMain       got hint locale=en_GB.UTF-8
10:37:44:0587 FuMain       Called GetPlugins()
10:37:44:0594 FuMain       Called SetFeatureFlags(63)
10:37:44:0597 FuMain       Called GetDevices()
10:37:44:0602 FuMain       Called GetHistory()
10:37:44:0629 FuMain       Called GetRemotes()

[0] 0:sh*
CTRL-A Z for help | 115200 8N1 | APP | Minicom 2.7.1 | VT102 | Offline | ttyS1
"pfSense.home.arpa" 10:37 28-Jan-22

```



OPNsense is an open-source, FreeBSD-based firewall and routing software developed by Deciso. Our proof of concept work was based on OPNsense 21.1, which is based on FreeBSD 12.1 with HardenedBSD patches

Hardware and software stack:

- PC Engines apu2 - Router/firewall board
- OPNsense 21.1
- fwupd 1.6.2

- Due to the fact that OPNsense and pfSense are FreeBSD based software, most of the pfSense PoC work could be directly moved to OPNsense
- OPNsense uses pkg as the package manager and supports the usual FreeBSD build facilities. The official repositories only contain a subset of upstream FreeBSD repositories
- Applying our fwupd port on top of the OPNsense ports tree works mostly without conflicts. It's possible to compile and run fwupd, with some plugins disabled

```
mkopec@mkopec ~> ssh root@192.168.122.151
Last login: Thu Jan 27 14:40:20 2022 from 192.168.122.1
-----
|      Hello, this is OPNsense 21.1      |      @@@@@@@@@@@@@@@@
|                                         |      @@@@          @@@@
| Website:   https://opnsense.org/      |      @@@\ \ \   //@@@
| Handbook:  https://docs.opnsense.org/ |      )))))))  (((((((
| Forums:    https://forum.opnsense.org/ |      @@@//   \ \@@@
| Code:      https://github.com/opnsense |      @@@@          @@@@
| Twitter:   https://twitter.com/opnsense |      @@@@@@@@@@@@@@@@
|-----|
root@OPNsense:~ # fwupdtool --version
client version: 1.6.2
compile-time dependency versions
gusb: 0.3.7

root@OPNsense:~ # █
```



Some issues needed solving before fwupd could compile and run:

- Running fwupdttool fails because the file `/etc/os-release` is missing. Creating one manually fixes the issue and lets fwupdttool run.
- On FreeBSD 12.1, including `<malloc.h>` causes the compiler to throw an error. Any instance of `<malloc.h>` needs to be replaced with `<stdlib.h>`. This was fixed in FreeBSD 13.0: <https://github.com/freebsd/freebsd-src/commit/bbbed78aaa9ad2d55ed30c15707e7efce92b80d1>
- Some parts are missing to compile fwupd with the UEFI support:
 - fwupd-efi needs compiling with gcc10, which isn't available in OPNsense repositories (compiling from ports is required)
 - ESRT support
 - efivar support

- Finding funding for the future work
- Fixing known issues
- Adding support for new fwupd plugins (UEFI capsule, flashrom plugin)
- Constant upstream of our work

The background is a dark gray color. In the corners, there are decorative elements consisting of light gray lines and circles, resembling a circuit board or a network diagram. These elements are positioned in the top-left, top-right, and bottom-right corners.

Thank you for your attention!