How to submit a CVE fix to the Yocto Project?

Marta Rybczynska, Syslinbit

Yocto Project Summit, 2023.11

I have an unpatched CVE...

- From the cve-check
- From monitoring of the new CVE stream
- As a part of a coordinated disclosure
- I implemented the fix upstream

I have an unpatched CVE...

- From the cve-check
- From monitoring of the new CVE stream
- As a part of a coordinated disclosure
- I implemented the fix upstream

Now what?

A few checks before you start….

- **Is there someone else working on it?**
  - Ask! Check the mailing list archives!
  - Check the proposal of a process at https://wiki.yoctoproject.org/wiki/Synchronization_CVEs
- **Is the backported patch to the version in YP available?**
  - Upstream first
  - Can check big distributions as Debian
  - Remember: we start applying from master (if versions match)
- **Which YP versions are affected?**

Patch naming

- **Example from dunfell's ffmpeg**
  https://git.openembedded.org/openembedded-core/tree/meta/recipes-multimedia/ffmpeg/ffmpeg_4.2.2.bb?h=dunfell

```
SRC_URI = "https://www.ffmpeg.org/releases/${BP}.tar.xz \
           file://mips64_cpu_detection.patch \
           file://CVE-2020-12284.patch \
           file://0001-libavutil-include-assembly-with-full-path-from-sourc.patch \
           file://CVE-2021-3566.patch \
           file://CVE-2021-38291.patch \
           file://CVE-2022-1475.patch \
           file://CVE-2022-3109.patch \
           file://CVE-2022-3341.patch \
           file://CVE-2022-48434.patch \
       "
```

Patch naming

- **Example from dunfell’s ffmpeg**
  https://git.openembedded.org/openembedded-core/tree/meta/recipes-multimedia/ffmpeg/ffmpeg_4.2.2.bb?h=dunfell

```
SRC_URI = "https://www.ffmpeg.org/releases/${BP}.tar.xz \
           file://mips64_cpu_detection.patch \
           file://CVE-2020-12284.patch \
           file://0001-libavutil-include-assembly-with-full-path-from-sourc.patch \
           file://CVE-2021-3566.patch \
           file://CVE-2021-38291.patch \
           file://CVE-2022-1475.patch \
           file://CVE-2022-3109.patch \
           file://CVE-2022-3341.patch \
           file://CVE-2022-48434.patch \
       "
```

Original patch header

- https://github.com/FFmpeg/FFmpeg/commit/9cf652cef49d74afe3d454f27d49eb1a1394951e.patch/

```
From 9cf652cef49d74afe3d454f27d49eb1a1394951e Mon Sep 17 00:00:00 2001
From: Jiasheng Jiang <jiasheng@iscas.ac.cn>
Date: Wed, 23 Feb 2022 10:31:59 +0800
Subject: [PATCH] avformat/nutdec: Add check for avformat_new_stream

Check for failure of avformat_new_stream() and propagate
the error code.

Signed-off-by: Michael Niedermayer <michael@niedermayer.cc>
---
 libavformat/nutdec.c | 16 ++++++++++++----
 1 file changed, 12 insertions(+), 4 deletions(-)
```

YP patch header

- https://git.openembedded.org/openembedded-core/tree/meta/recipes-multimedia/ffmpeg/ffmpeg/CVE-2022-3341.patch?h=dunfell

```
From 9cf652cef49d74afe3d454f27d49eb1a1394951e Mon Sep 17 00:00:00 2001
From: Jiasheng Jiang <jiasheng@iscas.ac.cn>
Date: Wed, 23 Feb 2022 10:31:59 +0800
Subject: [PATCH] avformat/nutdec: Add check for avformat_new_stream

Check for failure of avformat_new_stream() and propagate
the error code.

Signed-off-by: Michael Niedermayer <michael@niedermayer.cc>

CVE: CVE-2022-3341

Upstream-Status: Backport [https://github.com/FFmpeg/FFmpeg/commit/9cf652cef49d74afe3d454f27d49eb1a1394951e]

Comments: Refreshed Hunk
Signed-off-by: Narpat Mali <narpat.mali@windriver.com>
Signed-off-by: Bhabu Bindu <bhabu.bindu@kpit.com>
---
 libavformat/nutdec.c | 16 ++++++++++++----
 1 file changed, 12 insertions(+), 4 deletions(-)
```

In real life… the patch does not apply

- **Using devtool**
  - Remove the patch from SRC_URI
  - `devtool modify <recipename>`
  - Add the patch in the sources
  - Build/modify as needed, then commit
  - See: https://docs.yoctoproject.org/ref-manual/devtool-reference.html#

Check-list before sending

- Is it the correct patch for that issue?
- Does it build?
- Does it fix the issue? (if possible to verify)
- Do tests pass? (if available for the recipe)
- Have you started with the newest affected version?
- Does it apply to the head of the YP branch (eg. head of kirkstone)?

How to send

- Check the mailing list in the README of the layer
  - Other details available too
- Subscribe to the mailing list
- Send with git-send
- Monitor the ML for eventual comments
- Reply & fix if needed

If you're starting with Yocto Project

- Review https://docs.yoctoproject.org/contributor-guide/index.html
- Have a look at existing CVE fixes in related recipes
- If in doubt, ask (ML or IRC)

Summary

- **CVE fixes should follow a specific formalism**
  - patch file name
  - CVE tag in the header of the internal patch file
- **Common errors**
  - Version mismatches
  - Build failures

How to submit a CVE fix to the Yocto Project?

Marta Rybczynska, Syslinbit

Yocto Project Summit, 2023.11

yocto PROJECT

THE LINUX FOUNDATION