Remediating 1000s of untracked vulnerabilities in nixpkgs

delroth — FOSDEM 2024

CVE-2023-4863

“A buffer overflow in libwebp which allows a malicious actor to potentially get code execution in software that displays a specially crafted image file. This impacts pretty much all web browsers, as well as other software which might process or display untrusted images (image editing software, email clients, chat clients, social media clients, etc.). Chrome has rated this vulnerability as critical severity and has indicated that they have evidence some actors are already exploiting it in the wild.”

libwebp: cherry-pick suspected upstream fix for CVE-2023-4863

```
This CVE is critical severity and has been exploited in the wild. It was
reported as being a Chromium vulnerability, but it seems to in fact
impact libwebp (and thus all its downstream users). There is however no
official confirmation of this yet.

The upstream fix patch (webmproject/libwebp@902bc919) does not cleanly
apply onto 1.3.1, so we vendor a very slightly modified version which
does cleanly apply. This is my original work, so YMMV on whether you
trust it or not, reviews very much welcomed :-)
```

master (#254775)

24.05-pre ... 23.11-beta

delroth committed on Sep 12, 2023 Verified commit 0f11042876c07f1abbe172d9c8fe41feedd0be9c

361 pkgs/development/libraries/libwebp/CVE-2023-4863.patch

8 pkgs/development/libraries/libwebp/default.nix

Problem solved!

delroth commented on Sep 12, 2023 • edited by vcunat Member •••

Filing this issue to track CVE-2023-4863 related actions in nixpkgs. Feel free to send questions my way and/or contribute via comments in this issue!

Current status

Firefox and Chromium are not vulnerable anymore as of 2023-09-16 in `unstable` and `23.05`. Direct dependents of the system `libwebp` are also not vulnerable anymore. Some applications bundle their own version of libwebp instead of using the system version (including some other web browsers in nixpkgs: Brave, Tor Browser, etc.). Each of these need to be updated separately by nixpkgs maintainers. See below for a list of all the known applications that need an update and their status.

nixpkgs#254798

- [x] libwebp is updated in staging-next (unstable: libwebp: cherry-pick suspected upstream fix for CVE-2023-4863 #254775, 23.05: [staging-23.05] libwebp: cherry-pick suspected upstream fix for CVE-2023-4863 #254789)
  - [x] This will make it to master via staging-next 2023-09-07 #253854 - **@vcunat** said likely this weekend.
  - [x] We need to merge staging-23.05 to release-23.05. That should also finish this week: staging-next-23.05 iteration 8 - 2023-09-13 #254997
- [x] electron is also vulnerable. Upstream is making new releases on all their supported branches to include the patch.
  - [x] electron 26 bumped in master (electron: 26.1.0 -> 26.2.1 (CVE-2023-4863, #254798) #254816).
  - [x] electron 25 bumped in master (Electron 22/24/25 version bumps for CVE-2023-4863 #255069).
  - [x] electron 24 bumped in master (Electron 22/24/25 version bumps for CVE-2023-4863 #255069).
  - [x] electron 22 bumped in master (Electron 22/24/25 version bumps for CVE-2023-4863 #255069).
  - [x] electron 26 bumped in 23.05 ([Backport release-23.05] electron: 26.1.0 -> 26.2.1 (CVE-2023-4863, #254798) #254819).
  - [x] electron 25 bumped in 23.05 ([Backport release-23.05] Electron 22/24/25 version bumps for CVE-2023-4863 #255072).
  - [x] electron 24 bumped in 23.05 ([Backport release-23.05] Electron 22/24/25 version bumps for CVE-2023-4863 #255072).
  - [x] electron 22 bumped in 23.05 ([Backport release-23.05] Electron 22/24/25 version bumps for CVE-2023-4863 #255072).
- [ ] We should figure out what else might be vendoring libwebp. Not sure if there's tooling for this? List of derivations to investigate further and possibly patch:
  - List of stuff found to vendor libwebp + triaging status
  - [x] High risk stuff (mail clients, IM clients, web browsers)
    - [x] armcord
    - [x] caprine-bin (caprine-bin: 2.58.0 -> 2.58.3 #257372, [Backport 23.05] caprine-bin: 2.55.5 -> 2.58.3 #257472)
    - [x] discord (discord: 0.0.29 -> 0.0.30 #256943, [Backport release-23.05] discord: 0.0.29 -> 0.0.30 #256994)
      - [x] Darwin version: discord: Darwin updates #257496 / [Backport release-23.05] discord: Darwin updates #257716
    - [x] fluffychat (Backport all flutter & flutter package changes to 23.05 #257166)
    - [x] gitter (gitter: remove (unmaintained upstream, probably useless now) #255784, [release-23.05] gitter: mark vulnerable to CVE-2023-4863 #255786)
    - [x] mailspring
    - [x] mattermost-desktop (mattermost-desktop: 5.3.1 -> 5.5.0 #257162 / [Backport release-23.05] mattermost-desktop: 5.3.1 -> 5.5.0 #257243)
    - [x] mautrix-whatsapp (mautrix-whatsapp: 0.10.1 -> 0.10.2 #256178 / 23.05 [Backport release-23.05] mautrix-whatsapp: 0.10.1 -> 0.10.2 #256209)
    - [x] microsoft-edge (microsoft-edge: 116.0.1938.76 -> 117.0.2045.35 #256223 / [Backport release-23.05] microsoft-edge: 116.0.1938.76 -> 117.0.2045.35 #256595)
    - [x] mullvad-browser (mullvad-browser: 12.5.3 -> 12.5.4 #255078 / [Backport release-23.05] mullvad-browser: 12.5.3 -> 12.5.4 #255106)
    - [x] palemoon-bin (palemoon-bin: 32.3.1 -> 32.4.0.1 #257126, [Backport release-23.05] palemoon-bin: 32.3.1 -> 32.4.0.1 #257614)
    - [x] rocketchat-desktop (rocketchat-desktop: 3.8.11 -> 3.9.7 #255910 / [Backport release-23.05] rocketchat-desktop: 3.8.11 -> 3.9.7 #257128)
    - [x] signal-desktop (signal-desktop: 6.30.1 -> 6.30.2 #255129, [release-23.05] signal-desktop: 6.29.1 -> 6.30.2 (CVE-2023-4863, #254798) #255139)
    - [x] signal-desktop-beta (signal-desktop: 6.30.2 -> 6.31.0, signal-desktop-beta: 6.31.0-beta.1 -> 6.32.0-beta.1 #256435 / [Backport release-23.05] signal-desktop-beta: 6.30.0-beta.2 -> 6.31.0-beta.1, signal-desktop-beta: 6.31.0-beta.1 -> 6.32.0-beta.1 #257169)
    - [x] slack (slack: 4.34.115 -> 4.34.120 #257135 / [Backport release-23.05] slack: 4.29.149 -> 4.34.120 (linux), 4.29.149 -> 4.34.119 (darwin) #257149)
    - [x] threema-desktop (embedded electron not used)
    - [x] tor-browser-bundle-bin (tor-browser-bundle-bin: 12.5.3 -> 12.5.4 #255076 / [Backport release-23.05] tor-browser-bundle-bin: 12.5.3 -> 12.5.4 #255105)
    - [x] tutanota-desktop (tutanota-desktop: 3.115.2 -> 3.118.7 #255335 / [Backport release-23.05] tutanota-desktop: 3.112.6 -> 3.118.7 #255888)
  - [ ] Libs that other stuff might depend on
    - [x] flutter
    - [x] libcef (libcef: 116.0.21 -> 116.0.24 #256001 / [release-23.05] libcef: 112.3.0 -> 116.0.24 #256003)
    - [x] opencv (opencv3,opencv4: disable some unnecessary vendoring on Darwin #256444 / [Backport release-23.05] opencv3,opencv4: disable some unnecessary vendoring on Darwin #257726)
    - [x] qt5.qtimageformats (`libsForQt5.qt5.qtimageformats`: add dependencies `jasper`, `libmng`, and `libwebp` #255044 / [23.05] qt5.qtimageformats: unvendor libwebp #255432)
    - [ ] qtwebengine (darwin only, maybe?)
    - [x] smooth (smooth: unvendor all the things #255994 / [Backport release-23.05] smooth: unvendor all the things #256182)
  - [x] darktable (CVE-2023-4863 (libwebp heap buffer overflow) tracking #254798 (comment))
  - [x] golden-cheetah-bin: ships a vulnerable prebuilt libwebp (cc: **@gador** **@adamcstephens**)
    golden-cheetah-bin: mark insecure due to CVE-2023-4863 #255339
    [23.05] golden-cheetah-bin: mark insecure due to CVE-2023-4863 #258357
  - [ ] koreader: ships a vulnerable prebuilt libwebp (cc: **@contrun** **@neonfuz**)
  - [x] libreoffice (CVE-2023-4863 (libwebp heap buffer overflow) tracking #254798 (comment))
  - [ ] localsend: ships a vulnerable prebuilt libwebp (cc: **@sikmir**)
  - [ ] obs-studio (CVE-2023-4863 (libwebp heap buffer overflow) tracking #254798 (comment))
  - [ ] rigsofrods-bin (ships a vulnerable prebuilt libwebp (cc: **@wegank**))
  - [x] Anything Rust that depends (transitively or not) on libwebp-sys2 < v0.1.8
    - libwebp-sys2 might silently decide to build its vendored version, if it can't find system libwebp or if the `static` crate feature is enabled.
    - [x] gst_all_1.gst-plugins-rs (gst_all_1.gst-plugins-rs: check that system libwebp was linked #254915)
    - [x] catppuccin-catwalk (catppuccin-catwalk: use system libwebp #254911)
  - [x] Anything Rust that depends (transitively or not) on libwebp-sys < v0.9.3
    - Linking against system webp is intentionally not supported: Support linking to system-installed libwebp NoXF/libwebp-sys#17
    - [x] oculante (oculante: 0.7.4 -> 0.7.5 #255247
  - [ ] .NET software that uses SkiaSharp. Upstream has yet to release a fixed version. ([BUG] SkiaSharp vendors libwebp vulnerable to CVE-2023-4863 mono/SkiaSharp#2608)
    - [ ] avalonia-ilspy
    - [ ] BeatSaberModManager
    - [ ] denaro
    - [ ] galaxy-buds-client
    - [ ] jellyfin
    - [ ] mission-planner
    - [ ] mqttmultimeter
    - [ ] opentracker
    - [ ] openutau
    - [ ] ryujinx
    - [ ] scarab
    - [ ] wasabiwallet
  - [ ] Go software linking with https://github.com/chai2010/webp (CVE-2023-4863 impacting libwebp 1.0.2 chai2010/webp#61, Vendored libwebp is vulnerable to CVE-2023-4863 bep/gowebp#7) - broken down per vulnerable lib
    - [ ] https://github.com/chai2010/webp (unmaintained, likely never getting patched - action should be getting upstream to migrate away)
      - [x] hydron (hydron: mark as vulnerable to CVE-2023-4863 #255959 / [Backport release-23.05] hydron: mark as vulnerable to CVE-2023-4863 #256181)
      - [x] mautrix-whatsapp (mautrix-whatsapp uses an unmaintained webp library, vulnerable to CVE-2023-4863 mautrix/whatsapp#650)
    - [ ] https://github.com/bep/gowebp (Vendored libwebp is vulnerable to CVE-2023-4863 bep/gowebp#7)
      - [ ] hugo
  - [ ] Godot related derivations: these should be unvendored (capability already exists in the build system).
    - [ ] godot_4
    - [ ] godot3
    - [ ] godot3-server
    - [ ] godot3-headless
    - [ ] godot3-export-templates
    - Built using Godot
      - [ ] lorien
      - [ ] oh-my-git
  - [ ] Electron apps where we ship upstream binaries instead of using nixpkgs electron
    - Best course of action: upstream should update to electron >= 26.2.1, >= 25.8.1, >= 24.8.3, or >= 22.3.24 and tag a new release
    - [ ] atom
    - [ ] hakuneko
    - [ ] hyper
    - [ ] indigenous-desktop
    - [ ] joplin-desktop
    - [ ] keeweb (unmaintained, mark as insecure?)
    - [ ] keybase-gui
    - [ ] insomnia
    - [ ] mullvad-vpn
    - [ ] simplenote

Vendoring

delroth commented on Oct 2, 2023 Member Author •••

All the packages I evaluated as being high-risk have now been taken care of (and most of them did actually get updates, woo! only marked 2 or 3 as insecure). Right now I don't think anyone has the bandwidth to try and track the rest. I'm going to close this bug - if someone does want to take over the remediation for the rest of the impacted packages, feel free to reopen and assign yourself.

(Note however that there is a large overlap between vulnerable to this libwebp vuln and vulnerable to the recent libvpx vuln... so maybe just go help over there instead of reusing this bug.)

Packages containing…

libwebp copies in nixpkgs?	116
libpng copies in nixpkgs?	237
libjpeg copies in nixpkgs?	253
zlib copies in nixpkgs?	761

on nixpkgs-unstable, as measured on 2024-02-02,
unfree and insecure packages excluded

Is this a problem?

libpng per version

2	1.2.7
2	1.5.23
2	1.6.18
4	1.6.2
4	1.6.22
4	1.6.23
4	1.6.25
4	1.6.28
4	1.6.35
6	1.2.57
7	1.6.36
12	1.6.29

release date: 2004-09-12

release date: 2013-04-25

12	1.6.34
14	1.5.10
16	1.2.56
16	1.5.26
27	1.6.38
28	1.2.59
33	1.7.0
100	1.6.40
104	1.6.39
196	1.6.37

release date: 2012-03-29

Rust software analysis in nixpkgs

1844 Rust packages (has `cargoDeps`)

1149 locked to vulnerable dependencies (62%)

744 with high or critical severity vulnerabilities in dependencies (40%)

Some of it is nixpkgs's fault, most of it is upstream's fault...

What is causing vendoring?

➔ We don't try to prevent it.

➔ Newer language ecosystems encourage it.

➔ We don't have the tooling to detect and measure it.

Policies & Documentation

Packages fetched from AppImages: 58 (excl. unfree)

Packages fetched from .deb files: 66 (excl. unfree)

Many of these could be built from source, but it's harder!

nixpkgs does not currently document a preference for building from source. Some other distros do, famously Debian.

Rust, Go, NPM, Java, .NET

Lockfiles sound great, except upstream doesn't keep them up to date.

The shift towards lockfile-based language ecosystems mean distros have limited ways to fix vulnerable dependency. Upstreams don't understand this, or don't care.

- ➔ nixpkgs is special: huge package set, containing software that would in many distros be relegated to community / unofficial repos.
- ➔ Users should be made more aware of the risks: `knownVulnerable`, etc.

Tooling

Until recently, no tooling to detect or measure vendoring in nixpkgs.

In the wake of CVE-2023-4863: github:delroth/grep-nixos-cache

➢ Via simple signatures (currently, strings), find vendoring of common libs.

WIP: github:delroth/nixpkgs-vendored-vulns-scan

➢ Focusing on language specific ecosystems and lockfiles.

Conclusion

Conclusion

With new tooling, we have a better idea of the scale of vendoring in nixpkgs.

It's not great.

This talk does not come with any immediate solutions that can be applied. But a combination of policy changes, tooling improvement, and better support for informing users of the maintenance status of software will likely be necessary.

Questions & Contact Info

Github: delroth

Matrix: @delroth:delroth.net

Mastodon: @delroth@delroth.net

Email: delroth@delroth.net

github:delroth/grep-nixos-cache
github:delroth/nixpkgs-vendored-vulns-scan

Thank you!