Closed Issue created 6 months ago by **Adam Doupe**

matroska: heap overwrite in gst_matroska_demux_add_wvpk_header

Describe the vulnerability

The vulnerability is an integer overflow in `gst_matroska_demux_add_wvpk_header` which leads to a heap overwrite.

The allocation of `newbuf` can overflow so if `blocksize` is very large.

```
      newbuf =
          gst_buffer_new_allocate (NULL, WAVPACK4_HEADER_SIZE + blocksize,
          NULL);
```

https://gitlab.freedesktop.org/gstreamer/gstreamer/-/blob/main/subprojects/gst-plugins-good/gst/matroska/matroska-demux.c#L3980

Later in the function, memory is copied from our `data` to `outdata` (which is mapped from `newbuf`, and `blocksize` is used (which is very large)

```
memcpy (outdata, data, blocksize);
```

https://gitlab.freedesktop.org/gstreamer/gstreamer/-/blob/main/subprojects/gst-plugins-good/gst/matroska/matroska-demux.c#L4002

An interesting note is that this would be impossible to trigger because of the size check on blocks in `gst_matroska_demux_check_read_size`, which restricts ebml blocks to size `MAX_BLOCK_SIZE`: https://gitlab.freedesktop.org/gstreamer/gstreamer/-/blob/main/subprojects/gst-plugins-good/gst/matroska/matroska-demux.c#L5332

However, you can get around this by using zlib to decompress a block that is `< MAX_BLOCK_SIZE` into something much larger.

Expected Behavior

Not segfault.

Observed Behavior

Segfault.

Setup

- **Operating System:** Ubuntu 20.04.4
- **Device:** Computer
- **GStreamer Version:** 1.16.2

Steps to reproduce the bug

1. Download
2. Run `gst-play-1.0 ./wvpk-crash.mkv` wvpk-crash.mkv (note it takes awhile, roughly 20 seconds on my machine to crash).

How reproducible is the bug?

Always.

Impact

Heap overwrite. An attacker can survive the overwrite by careful massaging of the heap, and corrupt heap objects and heap metadata (I have done this part). This can lead to arbitrary code execution (although I have *not* done this part).

Additional Information

I'd like to request a CVE for this vulnerability.

Thank you, happy to help.

Drag your designs here or click to upload.

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Related merge requests 1

matroskademux: Avoid integer-overflow resulting in heap corruption in WavPack header handling code

!2612 1.21.1 ✓

When this merge request is accepted, this issue will be closed automatically.

Activity

Sebastian Dröge @slomo · 6 months ago Owner

0001-matroskademux-Avoid-integer-overflow-resulting-in-he.patch

This patch is fixing it by simply erroring out at that point if the addition would overflow. I've also changed the `blocksize` variable to a `size_t / gsize` for good measure.

Thanks for the analysis and reporting :)

OOC, why didn't you create a patch yourself? You already did all the hard work after all.

Edited by Sebastian Dröge 6 months ago

Tim-Philipp Müller added Security label 6 months ago

Tim-Philipp Müller @tpm · 6 months ago Owner

We'll probably merge these patches closer to the next stable bug-fix release %1.20.3 in ca. 2 weeks time or so.

It would be great if you could give us some indication whether you expect there to be more issues forthcoming in the near future (e.g. if you're running a lab at the moment that's still actively identifying problems), so we don't do a new bug-fix release and then 10 new issues come in the day after :)

Adam Doupe @adamdoupe · 6 months ago Author

@slomo I verified that the patch does indeed fix the issue. I didn't write a patch because I didn't know what approach you'd all like to use to fix it, but I can do that for the remaining issues.

@tpm I have about four more vulnerabilities to report, however I don't have POCs at the moment for them. I'll get those in ASAP, and I'll mention in my last report that it's the last that I have.

Sebastian Dröge @slomo · 6 months ago Owner

> @slomo I verified that the patch does indeed fix the issue. I didn't write a patch because I didn't know what approach you'd all like to use to fix it, but I can do that for the remaining issues.

As you prefer :) If you're unsure about the approach to fix an issue then that's also fine and we can take care of that, it's just that you basically wrote the patch in words here

Sebastian Dröge @slomo · 6 months ago Owner

Oh one thing to keep in mind if you want to submit the changes yourself is that it's not possible create a confidential merge request with the GitLab community edition. So it has to be an issue with an attached patch, like here, unfortunately.

Adam Doupe @adamdoupe · 6 months ago Author

Hi @slomo and @tpm, I reported the issues that I found that are highly likely to be exploitable to Red Hat's CNA for CVEs.

This issue "heap overwrite in gst_matroska_demux_add_wvpk_header" is CVE-2022-1920.

I'll post updates on the other issues as well.

Tim-Philipp Müller @tpm · 5 months ago Owner

Patch looks OK to me.

I wonder if we shouldn't enforce a smaller sanity check on the wavpack blocksize here anyway though.

Sebastian Dröge @slomo · 5 months ago Owner

Probably not the worst idea. How much would you say? 120MB?

Tim-Philipp Müller @tpm · 5 months ago Owner

> Probably not the worst idea. How much would you say? 120MB?

Seems reasonable. I think the actual allowed blocksize is 1MB or so, so seems safe enough.

On the other hand we could just leave it so we don't inadvertently cause problems.

Tim-Philipp Müller changed milestone to %1.20.3 5 months ago

Sebastian Dröge mentioned in commit `tpm/gstreamer@1278cd12` 5 months ago

Sebastian Dröge mentioned in commit `tpm/gstreamer@f07d90a4` 5 months ago

Tim-Philipp Müller mentioned in merge request !2612 (merged) 5 months ago

Sebastian Dröge mentioned in commit `tpm/gstreamer@061cd9c2` 5 months ago

Sebastian Dröge mentioned in commit `tpm/gstreamer@e93d02d0` 5 months ago

Sebastian Dröge mentioned in commit `tpm/gstreamer@df49be03` 5 months ago

Sebastian Dröge mentioned in commit `tpm/gstreamer@0df0dd7f` 5 months ago

Sebastian Dröge mentioned in commit `tpm/gstreamer@f5fd8195` 5 months ago

Sebastian Dröge mentioned in commit `tpm/gstreamer@cf887f1b` 5 months ago

Sebastian Dröge closed via commit `cf887f1b` 5 months ago

Tim-Philipp Müller made the issue visible to everyone 5 months ago

Sebastian Dröge mentioned in commit `wtaymans/gstreamer@c10a9d55` 2 weeks ago

Please register or sign in to reply