

New issue

Jump to bottom

## Ebml[Unicode]String::ReadData heap overflow bug on 32bit builds #74

 Closed kryc opened this issue on Feb 7, 2021 · 4 comments · Fixed by #76

Assignees



Labels

bug

kryc commented on Feb 7, 2021

### --[ 1. Summary

An extremely exploitable heap overflow bug exists in the implementation of EbmlString::ReadData and EbmlUnicodeString::ReadData in libebml. This bug is reachable from the current stable release of vlc.

### --[ 2. Discussion

The issue exists in the calculation of the required buffer size to store the string. The following calculation is performed:

```
310      auto Buffer = new (std::nothrow) char[GetSize()+1];
...
315      input.readFully(Buffer, GetSize());
```

The value returned from GetSize is guaranteed to be an unsigned 64 bit number, and due to the way in which integers are stored and parsed in Ebml will only use the lowest 48 bits. This guarantees that the integer cannot overflow on 64bit builds.

However, on 32bit builds, the value is implicitly cast to a size\_t in the call to new, meaning that the truncated length can be significantly shorter than the amount of data to be copied. For example, if the length of the string element is claimed to be 0xffffffff, the resultant allocation will be 0x100000000. The cast to a 32bit size\_t drops the top 1 bit, meaning an array of size zero is allocated.

In the event that the string element is placed maliciously at the end of the file to be parsed, an extremely exploitable controlled heap overflow can occur.


### --[ 3. Resolution

The fix for this bug is relatively straightforward, a check must be added to ensure that the value of GetData() + 1 is less than SIZE\_MAX to ensure that it will not be truncated in the call to new.

### --[ 4. Proof of Concept

The following proof of concept file shows the behaviour in the latest (at time of writing) version of vlc on Ubuntu 10.10.

```
$ sudo apt install vlc:i386 gdb
$ wget https://kryc.uk/libebml-poc.mkv
$ gdb -q vlc
$$ r libebml-poc.mkv
```

 kryc mentioned this issue on Feb 7, 2021

Add fix for heap buffer overflow bug on 32bit builds #75


 Closed

 mbunkus added the bug label on Feb 7, 2021

mbunkus commented on Feb 7, 2021

Contributor

Thank you very much! I'll likely prepare a new release tomorrow.

 mbunkus self-assigned this on Feb 7, 2021

carnil commented on Feb 10, 2021

This issue was assigned CVE-2021-3405

 robUx4 mentioned this issue on Feb 11, 2021

Fix misc reading overflows #76

➔ Merged

 mbunkus closed this as completed in #76 on Feb 18, 2021

mbunkus commented on Feb 18, 2021

Contributor

As written in #76:

I've just spent a couple of hours building current libebml with this PR, current libmatroska & VLC on Debian 10 (as there are no 32-bit installation images for Ubuntu anymore). Debian's VLC with Debian's libebml/libmatroska crashes as expected; the re-built ones don't — only a couple of error messages from VLC's Matroska plugin. Meaning the fix seems to work as far as I can tell.

I'll package a new release of libebml later today.

mbunkus commented on Feb 18, 2021

Contributor

libEBML v1.4.2 & libMatroska v1.6.3 are out:

<https://www.matroska.org/downloads/libraries.html>

The former is solely the bug fix for this issue; the latter solely adding new classes for track header flags.



Assignees

 mbunkus

Labels

bug

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 Fix misc reading overflows  
Matroska-Org/libebml

3 participants

