

[New issue](#)[Jump to bottom](#)

electron crash, needs at least input validation for pdfstreamresponse #439

✓ Closed

julianhille opened this issue on Oct 18, 2019 · 1 comment

julianhille commented on Oct 18, 2019

Contributor

```
"electron": "4.2.9",  
"hummus": "^1.0.105",
```

Reproduce is as simple as this:

```
hummus = require('hummus')  
writer = new hummus.PDFStreamForResponse(null)  
writer = hummus.createWriter(writer)  
writer.end()
```

The object `PDFStreamForResponse` does take ANYTHING as value.

This later will be used to write the header to int and so goes through `WriteComment` in `hummus`.

The node/electron call to `v8::V8::ToLocalEmpty` kills it and jumps bad in memory.

Parts of the stack to follow:

```
Thread 0 Crashed:: CrBrowserMain Dispatch queue: com.apple.main-thread  
0  com.github.Electron.framework 0x00000001069702f0 0x104c13000 + 30790384  
1  com.github.Electron.framework 0x0000000106397560 v8::V8::ToLocalEmpty() + 64  
2  hummus.node 0x000000010e2fcff1  
ObjectByteWriterWithPosition::Write(unsigned char const*, unsigned long) + 615  
3  hummus.node 0x000000010e33cfed  
ObjectsContext::WriteComment(std::__1::basic_string<char, std::__1::char_traits<char>,  
std::__1::allocator<char> > const&) + 35  
4  hummus.node 0x000000010e320c49  
PDFHummus::DocumentContext::WriteHeader(EPDFVersion) + 23  
5  hummus.node 0x000000010e2f34bc  
PDFWriterDriver::StartPDF(v8::Local<v8::Object>, EPDFVersion, LogConfiguration const&,  
PDFCreationSettings const&) + 90  
6  hummus.node 0x000000010e2fd4c4  
CreateWriter(v8::FunctionCallbackInfo<v8::Value> const&) + 2778``
```

Could be easily fixed if at least some null / undefined checks are done here.



julianhille closed this as completed on Jun 28

julianhille commented on Jun 28

Contributor

Author

[julianhille/MuhammaraJS#188](#)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

