

# Security Examples Hyperlinks

Caolán McNamara

Principal Software Engineer

caolan.mcnamara@collabora.com



Collabora  
Online



Technical Day  
COOL  
days





# CVE-2023-6186

## Link targets allow arbitrary script execution

- LibreOffice supports hyperlinks, typical http[s] protocol
  - <https://www.collaboraoffice.com/>
- There can be hyperlinks in document text and in editing text, etc
- And Calc has a =HYPERLINK(someURL) function



# CVE-2023-6186

## Scripts and Macros

- Tend to use “Macro” for executable content that is bundled into a document
- Tend to use “Script” for executable content that is part of the application

## Traditionally warned just about “Macros” in the document

- But assume that “Scripts” that are part of the application are “safe”
- So didn’t get warnings that a document could run a built-in script in some way if it didn’t contain macros of its own
  - e.g. bind to document events



# CVE-2023-6186

## Flaws in allowing scripts to be run

- CVE-2018-16858 Directory traversal flaw in script execution
- CVE-2019-9848 LibreLogo arbitrary script execution
- CVE-2019-9852 Insufficient URL encoding flaw in allowed script location check
- CVE-2019-9851 LibreLogo global-event script execution
- CVE-2019-9850 Insufficient url validation allowing LibreLogo script execution
- CVE-2019-9853 Insufficient URL decoding flaw in categorizing macro location
- CVE-2019-9855 Windows 8.3 path equivalence handling flaw allows LibreLogo script execution
- CVE-2019-9854 Unsafe URL assembly flaw in allowed script location check



# CVE-2023-6186

## Too many ways to execute things without bundling macros

- Just rule that calling bundled scripts is hazardous
  - LibreLogo, ScriptForge, example scripts
- So expand warning/lock-down to include calls to scripts/macros
- Not just bundling macros in the document
- Warning shown and scripting disabled if the document can call anything, even if that was considered safe in the past
- For better or worse, we have never warned if the user adds and runs script events during a session. Only on document load.



# CVE-2023-6186

## Back to Hyperlinks

- There are other exotic protocols that are possible, some of them LibreOffice specific
- `vnd.sun.star.script:Something`
- `.uno:Something`, `.slot:ID`, etc
- So, despite having warnings/lock-down for calling scripts, allowing hyperlinks to be dispatched allows these exotic protocols to be used to call scripts
- Amazingly this was fairly widely known, though not to me
  - <https://ask.libreoffice.org/t/assign-a-macro-to-a-cell-click/49171>



# CVE-2023-6186

**Other more exotic protocols exist, some LibreOffice specific**

- I still find it hard to believe this was a deliberate explicit choice
- You can even chain them
- `=HYPERLINK(".uno:OpenHyperLink?URL:string=macro%3a%2f%2f%2fImportWizard.Main.Main()")`
  - Calc hyperlink that dispatches “.uno:OpenHyperlink” with an argument of `macro://ImportWizard.Main.Main()`
  - Where OpenHyperlink then dispatches `macro:///...`



# CVE-2023-6186

## Ctrl+Click

- Well, at least you have to ctrl+click to activate these:
  - Since tdf#51296 "Ctrl-click required to follow hyperlinks"?
- No, because there was a bug logged after that effort, tdf#70959
- Explicit complaint that clicking on a calc HYPERLINK that had a macro target no longer worked
  - So while a plain click in writer without ctrl doesn't launch a hyperlink a plain click in calc on a =HYPERLINK cell does.





# CVE-2023-6186

## Resolution

- Centralize calc/writer/impress/etc user hyperlink interaction to run everything through a new `AllowedLinkProtocolFromDocument` which prompts (defaulting to no) for exotic protocols so the apparent use-case for calc hyperlink is still possible, but not without a warning dialog
  - Warning dialog auto returns no for online
- Remove the support for “exotic” protocols’ to appear as the link source for “Floating Frames”, another vector for use of obscure feature that could do things no one ever explicitly intended


- Thanks to Reginaldo Silva of [ubercomp.com](http://ubercomp.com) for reporting
- Thanks to Eike Rathke for calc insights



Collabora  
Online



LibreOffice Technology

*Technical Day*  
**COOL**  
*days* 

# Thank you!



@CollaboraOffice  
[hello@collaboraoffice.com](mailto:hello@collaboraoffice.com)  
[www.collaboraoffice.com](http://www.collaboraoffice.com)