First of all I want to clarify, that presented vulnerabilities are triggering RCE (Remote Code Execution) with user action (e.g. according to social engineering) or third party software changing contents of handlers.json(%APPDATA%\Mozilla\Firefox\Profiles\Here is your profile id\handlers.json) or about:config

The first vulnerability caused by poor filtration of executable files -

Example 1. Downloading malicious executable file, calc.exe.



As you can see, we can only “Save File” or “Cancel” download. If we save our file, it gets marked as malicious, everything Ok. Because we downloaded an .exe file, we are also getting “Google Safe Browsing” request, containing information about our calc.exe.



And here is vulnerability: If we change the name of calc.exe to exe.calc.txt , it is still an executable file, that might be executed, for example, via conhost. Let’s try to download it!

Example 2. Downloading malicious executable file calc.exe , renamed to exe.calc.txt



Now we are not only getting opportunity to instantly execute our malicious file, but we are also not triggering any of security checks.



Proof of Concept:

As an example of remote code execution. I will execute our malicious calc starter.

\*\*\* Watch 1st video! \*\*\*

If you stop vid on early 5 sec, you will see, that we are laucnhing our malware in local\temp directory. To actually execute our file using conhost.exe, we have three ways:

1) Simply select “Open with” and manually add there “C:\Windows\System32\conhost.exe”, then press OK and malicious code is executed.



2) Change “C:\Windows\System32\conhost.exe” as a default action for .txt files; Same result.



3) Edit %APPDATA%\Mozilla\Firefox\Profiles\Here is your profile id\handlers.json file; The same result. I also think it’s possible to edit using about:config.

But what if I say, that by using three last methods, you might execute any of cmd, powershell and etc code in browser, by simple click on the link in firefox?) That’s for real. Problem with opening exe.filename.txt is that you can not get rid of this window, where user needs manually select conhost or any other method; even if you change it in handlers.json or browser settings, process is not automatic and requires user to press “ok”. But not with magnet links!

Proof of Concept:

\*\*\* Watch 2nd video! \*\*\*

As you can see, we are running in C:\Windows\System32 directory.

In this case I used hyperlink <a href="magnet:?xt=/k calc.exe">click</a>,

Where magnet:?xt=/k calc.exe - magnet link: “megnet:?xt=” - association link as magnet; and “/k calc.exe” - any code, associated with our execution method

To make magnet links hanlde with any app you want (in our case C:\Windows\System32\cmd.exe), you need to modify highlighted string in handlers.json (or if there is no handlers for manget, you need to add this string) I also think it’s possible to do using about:config.



Remedy: For the downloading unsafe files – adjust .extension checking mechanism by associating exe.file.txt as file.exe etc.

For the system commands execution – disallow choosing important system commands as handlers for downloaded files; or disallow it at all (make it automatic, as It implemented in chrome, for example. Or link it to the default system file association)