./ persistence-info.github.io

View on GitHub

hhctrl.ocx

Location:

`HKCR\CLSID\{52A2AAAE-085D-4187-97EA-8C30DB990436}\InprocServer32`

Classification:

Criteria	Value
Permissions	Admin
Security context	User
Persistence type	Registry
Code type	Other[1]
Launch type	User initiated[2]
Impact	Destructive[3]
OS Version	All OS versions
Dependencies	OS only
Toolset	Scriptable

Description:

> When hh.exe is started it tries to find the hhctrl.ocx library by checking the following Registry value: `HKCR\CLSID{52A2AAAE-085D-4187-97EA-8C30DB990436}\InprocServer32’ The library that the value points to is then loaded. If the library doesn’t exist, or the loading didn’t succeed the hh.exe gives it another go and attempts to load the library using the hard-coded name hhctrl.ocx and relying on the LoadLibrary function (and as a result is a subject to side-loading attacks). As such, there seem to be at least 2 opportunities here:
>
> 1. Drop c:\WINDOWS\hhctrl.ocx and delete the HKCR\CLSID{52A2AAAE… value so running hh.exe will sideload the c:\WINDOWS\hhctrl.ocx
> 2. Replace the value of the HKCR\CLSID{52A2AAAE… to point to your own lib and run hh.exe – this will load the lib of choice

References:

https://www.hexacorn.com/blog/2018/04/23/beyond-good-ol-run-key-part-77/

Credits:

@Hexacorn

See also:

.chm helper DLL

Remarks:

1. .ocx ↩

2. ‘hh.exe’ must be run. Manually, or via associated .chm file ↩

[3] To be verified ↩