Brad Voris

Executive & Security Professional at Cyber Forge Security, Inc.

June 12, 2018updated June 12, 2018last reply June 21, 2018443 views

SettingContent-MS File Execution Vulnerability Exploit

This reminds me a lot of .HTA file exploitation (just not as scripted). It is a relatively new vulnerability that has been identified but does have potential of being extremely malicious.

https://posts.specterops.io/the-tale-of-settingcontent-ms-files-f1ea253e4d39

In Windows 10 this could be an easy compromise with Internet Explorer installed.

Furthermore on potential for malicious use:

Line 6 of the original code:

<DeepLink>%windir%\system32\cmd.exe /c calc.exe</DeepLink>

Replace with:

<DeepLink>%windir%\system32\cmd.exe /c "C:\Program Files\Internet Explorer\iexplore.exe" -k https://www.peerlyst.com </DeepLink>

This modification now automatically opens Internet Explorer, goes to the specified site and maximizes to the screen. With existing vulnerabilities in Internet Explorer it would be a cake walk for this to be exploited and deploy a malicious payload from an online source.

Github Repo:

https://github.com/bvoris/SettingContent-MS-File-Execution