

Forum: [Hack Forums](#)

Thread: [Implementing UAC bypass on most Windows system](#)

Forc?d - May 18, 2017, 4:40 pm

Just wanted to referee to some UAC methods discovered/disclosed by
<https://enigma0x3.net/>

Everything you need to implement some easy UAC bypass methods for whatever project you may need it to.

I may end-up posting implementation for some of these methods in VB.net if i feel bored

Most recent WIN10 uac bypass:

<https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/>

Enjoy! :)

ForceJew - May 19, 2017, 1:14 pm

Oh he is the guy who found eventviewer.
Guess he made another one.

Mr. Robot - May 19, 2017, 1:18 pm

Awesome that he put this at the bottom

This particular technique can be remediated or fixed by setting the UAC level to "Always Notify" or by removing the current user from the Local Administrators group. Further, if you would like to monitor for this attack, you could utilize methods/signatures to look for and alert on new registry entries in HKCU:\Software\Classes\exefile\shell\runas\command\isolatedCommand