



Settings



Post



Philip Tsukerman  
@PhilipTsukerman



1.5 #LOLBins not yet in @Oddvarmoe 's repository are Register-CimProvider and "msiexec /y" and "/z" (I count this as half, as this is just additional msiexec functionality). Both of these allow you to load an arbitrary dll.

```
Microsoft Windows [Version 10.0.16299.371]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\philip>msiexec /y "C:\Users\philip\Desktop\runcalc\x64\Release\runcalc.dll"

C:\Users\philip>Register-CimProvider -Path "C:\Users\philip\Desktop\runcalc\x64\Release\runcalc.dll"
'Namespace' is not specified.
'ProviderName' is not specified.
'MI_Main' is not exported by provider 'C:\Users\philip\Desktop\runcalc\x64\Release\runcalc.dll'.

Try 'Register-CimProvider.exe -help' for help.

C:\Users\philip>
```



2:41 PM · May 3, 2018

14 Reposts 37 Likes 4 Bookmarks



4



Don't miss what's happening

People on X are the first to know.

Log in

Sign up

Welcome to x.com!



We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same.  
For more details, see our Privacy Policy: <https://x.com/en/privacy>.

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. [Show more about your choices.](#)

Accept all cookies

Refuse non-essential cookies