



Search

Login

Sign up



Explore

My Profile

My Wallet

UAC Bypassing Utility



ah101 (51) in #utopian-io • 7 years ago (edited)

UAC Bypassing Utility

This is a project used in my R.A.T Client to bypass the UAC. It bypasses the UAC using a fake dismCore.dll that gets loaded by an auto elevating application. Then the dll starts my client and the client gets elevated too.

Disclaimer

This application is for educational purposes only.
Using this tool without understanding how it's working can lead to negative consequences.
I'm not responsible for the consequences of using this tool.
Only run it on a computer you have permission to!

How it works

Using an elevated COM object vulnerability we're able to copy files to protected locations like System32. pkgmgr.exe an auto elevating process calls dism.exe, which has a DLL hijacking vulnerability. So dism.exe calls our rogue dll which loads the given application. How does our dll know the location of our application? I solved it this way: Before executing the bypass a file containing the path to execute will be dropped to the Temp folder. This way the DLL can read out the path of the file, and

execute it. Because of the way windows is designed an elevated application by default executes another application elevated too! So now we bypassed the UAC.

What's dll hijacking

DLL hijacking is a vulnerability where we can trick an application to load our rogue DLL instead of the original one. The vulnerability exists, because the applications specify a `relative` path to load the DLL. The order of the checked directories for the DLL can be located in the PATH environment variable. The system basically finds our rogue dll in System32 before it checks the working directory of the launching application `dism.exe`

Technology Stack

Most of the code is c/c++. The launcher, which executes the bypass procedure is writtern in c#. The code was developed in Visual Studio 2017, the c# project is built with .NET 4.5.2. The architecture of the programs are really important, on a 32 bit machine only the x86 version of the toolkit will work. This is why I needed a custom launcher.

Future of this project

- Add support to launch any application after the bypass. Currently hard coded to launch my client
- I would appreciate if someone could test this on more systems. It's currently working on Win7 x64 without AV
- Drop back original DLL after bypass

How to contribute

Fork the project, make changes and issue a pull request. This is your part, then I will merge/edit the pull request. I will try to respond as fast as i can.

Summary

Got intrested? You can check out the project on github!
Thank you for checking out the project!

Posted on [Utopian.io - Rewarding Open Source Contributors](#)

#uacbypass #hacking #c #windows

🕒 7 years ago in #utopian-io by **ah101** (51) ▼

⬆️ ⬇️ \$97.57 ▼ 24 votes ▼

🔗 Reply 9     

Sort: [Trending](#) ▼



utopian-io (71) ▼ 7 years ago

[-]

Hey [@ah101](#) I am [@utopian-io](#). I have just upvoted you!

Achievements

- You have less than 500 followers. Just gave you a gift to help you succeed!
- This is your first accepted contribution here in Utopian. Welcome!

Community-Driven Witness!

I am the first and only Steem Community-Driven Witness. [Participate on Discord](#).
Lets GROW TOGETHER!

- [Vote for my Witness With SteemConnect](#)
- [Proxy vote to Utopian Witness with SteemConnect](#)
- Or vote/proxy on [Steemit Witnesses](#)

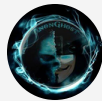
Witness Voting

You have 3 votes remaining. You can vote for a maximum of 30 witnesses.

	Witness	Information
01	jesta	witness thread
02	timcliff	witness thread
03	gtg	witness thread
04	roelandp	witness thread
05	blocktrades	witness thread
06	someguy123	witness thread
07	good-karma	witness thread
08	clayop	witness thread
09	smooth witness	witness thread

Up-vote this comment to grow my power and help Open Source contributions like this one. Want to chat? Join me on Discord <https://discord.gg/Pc8HG9x>

\$ 0.00 | 1 vote ▼ | Reply



ah101 (51) ▼ 7 years ago

[-]

Oh My.....

Thank You!!

\$ 0.00 | Reply

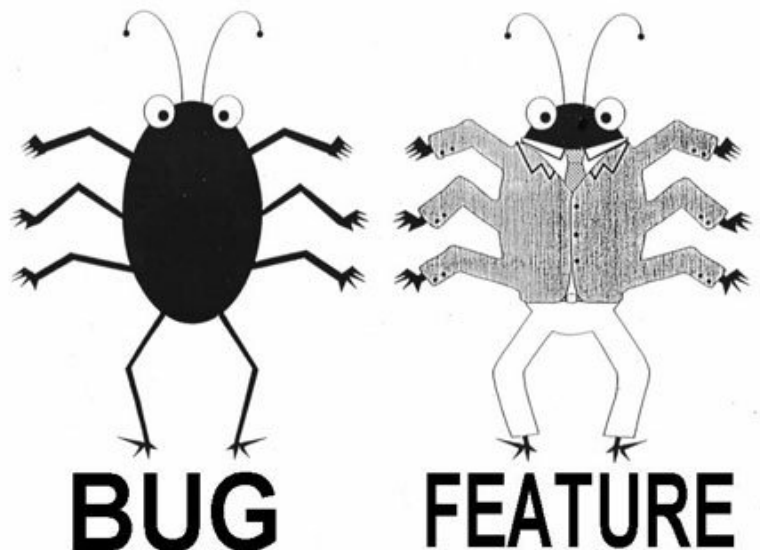


egodust (41) ▼ 7 years ago

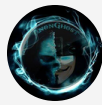
[-]

This is very educational and can help to teach people about information security so thanks for sharing.

I agree that technology is neutral and can be used for good or evil. A larger question is why doesn't Micro\$oft fix their UAC vulnerability so their UAC technology protects all users? There must be a way to fix this on their side?



  \$ 0.00 | 1 vote ▼ | Reply



ah101 (51) ▼ 7 years ago

[-]

Well the vulnerability isn't microsoft specific, at least DLL hijacking. DLL hijacking can be a vulnerability in any application! As for the elevated IFileOperation, which can copy files to System32 (which only admin users should be able to do), it is microsoft related, so they should fix that. And in this case the DLL hijacking vulnerability is present in a default microsoft application, so they should fix that too.



Also I didn't note in this post that this should only work with an administrator user's account.

So if a normal user logs in they need the admin account's password to deal with the UAC prompt. In this case the vulns are still present, but AutoElevate doesn't kick in for a regular user (most home PCs are running under an administrator account).

Also my *conspiracy theory* is that microsoft doesn't patch these below Win10 to attract more users from Win7, 8, 8.1 to the new Win10. But this is only a theory since I don't know how the tool performs on a Win10 system!

And yes this can be fixed on their side, most easily by specifying the absolute path of the DLL they can fix the DLL hijacking vulnerability. If any of the vulnerabilities used in the tool are fixed, then the tool just won't work.

I hope this answers some of your questions!

  \$ 0.00 | Reply



egodust (41) ▼ 7 years ago

[-]

Thanks for detailed explanation, this is good stuff thanks for your contribution.

  \$ 0.00 | Reply



helo (70) ▼ 7 years ago

[-]

Thank you for the contribution. It has been approved.

This post is very educational, you explain the concept in just the right amount of words.

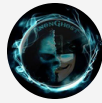
Please add a note to the post and your repo only for that the information is for educational purposes any bad use of it can lead to consequences.

A more standard license might be preferred.

You can contact us on [Discord](#).

[\[utopian-moderator\]](#)

  \$ 0.00 | Reply



ah101 (51) ▾ 7 years ago [-]



Thank you for the positive response!
Added disclaimers to both the post and the repo on github, and changed my crappy license to the *MIT License*

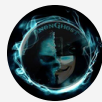
  \$ 0.02 ▾ | 1 vote ▾ | Reply



mys (62) ▾ 7 years ago [-]

This is evil

  \$ 0.00 | Reply



ah101 (51) ▾ 7 years ago (edited) [-]

As once google said



Don't be evil... (unless it's profitable)

Please don't take it seriously, I like google, they invent great stuff!

  \$ 0.00 | 1 vote ▾ | Reply