

Rundll32 and Phantom DLL lolbins

 hexacorn.com/blog/2024/09/03/rundll32-and-phantom-dll-lolbins

2024-09-03

This may be a new, kinda ephemereal addition to the lolbin world (not sure if anyone covered it before).

Windows 11 comes with a large number of DLLs – some of which are broken.

DuCsps.dll on Windows 11 Pro 22H2

The *DuCsps.dll* imports 2 APIs from *UpdateAPI.dll*:

- *GetInstalledPackageInfo*, and
- *FreeInstalledPackageInfo*.

The problem is that there is no *UpdateAPI.dll*. It may be present in other versions of Windows, but it's not present in 22H2 (note: I have not tested all the subversions, so YMMV).

tssrvlic.dll on Windows 11 Pro 22H2

The same goes for *tssrvlic.dll* that imports 3 APIs from a non-existing *TlsBrand.dll*:

- *RDSGetProductAccessRights*,
- *W2K3ADPUCALDetailsCreator*, and
- *RDSProductDetailsCreator*

They both create a lolbin opportunity via a missing phantom DLL, and an attacker can simply bring in their versions of malicious *UpdateAPI.dll* or *TlsBrand.dll*, and then run (from the same directory where these payloads are located) the following rundll32 commands:

```
rundll32 DuCsps.dll, foo
```

```
rundll32 tssrvlic.dll, bar
```

where *foo* and *bar* can be anything.

See below:

```
C:\test>rundll32 DuCsp.dll, foo_
```

#	Time	Debug Print
---	------	-------------