

# Regsvcs on LOLBAS

Archived: 2026-04-06 00:23:15 UTC

## .. /Regsvcs.exe

Regsvcs and Regasm are Windows command-line utilities that are used to register .NET Component Object Model (COM) assemblies

### Paths:

- C:\Windows\Microsoft.NET\Framework64\v2.0.50727\RegSvcs.exe
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
- C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
- C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

### Resources:

- <https://pentestlab.blog/2017/05/19/applocker-bypass-regasm-and-regsvcs/>
- <https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/>
- <https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.009/T1218.009.md>

### Acknowledgements:

- Casey Smith (@[subtee](#))

### Detections:

- Sigma: [proc\\_creation\\_win\\_lolbin\\_regasm.yml](#)
- Elastic: [execution\\_register\\_server\\_program\\_connecting\\_to\\_the\\_internet.toml](#)
- Splunk: [detect\\_regsvcs\\_with\\_network\\_connection.yml](#)

## Execute

1. Loads the target .NET DLL file and executes the RegisterClass function.

```
regsvcs.exe file.dll
```

Use case

Execute dll file and bypass Application whitelisting

Privileges required

User

## Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

## ATT&CK® technique

[T1218.009: Regsvcs/Regasm](#)

## Tags

Execute: DLL (.NET)

# AWL bypass

1. Loads the target .NET DLL file and executes the RegisterClass function.

```
regsvcs.exe file.dll
```

## Use case

Execute dll file and bypass Application whitelisting

## Privileges required

Local Admin

## Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

## ATT&CK® technique

[T1218.009: Regsvcs/Regasm](#)

## Tags

Execute: DLL (.NET)

---

Source: <https://lolbas-project.github.io/lolbas/Binaries/Regsvcs/>