

.. /Regsvcs.exe

Execute (DLL, Custom Format)

AWL bypass (DLL, Custom Format)

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: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_lolbin_regasm.yml
- Elastic: https://github.com/elastic/detection-rules/blob/12577f7380f324fcee06dab3218582f4a11833e7/rules/windows/execution/register_server_program_connecting_to_the_internet.toml
- Splunk: https://github.com/splunk/security_content/blob/bee2a4cefa533f286c546cbe6798a0b5dec3e5ef/detections/endpoint/detect_regsvcs_with_network_connection.yml

Execute

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

regsvcs.exe AllTheThingsx64.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
Tags:	Execute: DLL Input: Custom Format

AWL bypass

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

```
regsvcs.exe AllTheThingsx64.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
Tags:	Execute: DLL Input: Custom Format