.. /Regasm.exe ☆ Star 7,060

AWL bypass (DLL, Custom Format) Execute (DLL, Custom Format)

Part of .NET

Paths:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\regasm.exe
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\regasm.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: suspicious_regsvcs_regasm_activity.md
- Splunk: detect_regasm_with_network_connection.yml
- IOC: regasm.exe executing dll file

AWL bypass

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

```
regasm.exe AllTheThingsx64.dll
```

Use case:	Execute code 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 Input: Custom Format

Execute

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

```
regasm.exe /U AllTheThingsx64.dll
```

Use case:	Execute code 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 Input: Custom Format