.. /Pcwrun.exe

☆ Star 7,060

Execute

Program Compatibility Wizard

Paths:
C:\Windows\System32\pcwrun.exe

Resources:

- https://twitter.com/pabraeken/status/991335019833708544
- https://twitter.com/nas_bench/status/1535663791362519040

Acknowledgements:

- Pierre-Alexandre Braeken (@pabraeken)
- Nasreddine Bencherchali (@nas_bench)

Detections:

- Sigma: proc_creation_win_lolbin_pcwrun_follina.yml

Execute

1. Open the target .EXE file with the Program Compatibility Wizard.

```
Pcwrun.exe c:\temp\beacon.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:	**T1218**: System Binary Proxy Execution

2. Leverage the MSDT follina vulnerability through Pcwrun to execute arbitrary commands and binaries. Note that this specific technique will not work on a patched system with the June 2022 Windows Security update.

```
Pcwrun.exe /../../$(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**: Indirect Command Execution