

# /msedgewebview2.exe

Execute

msedgewebview2.exe is the executable file for Microsoft Edge WebView2, which is a web browser control used by applications to display web content.

## Paths:

C:\Program Files (x86)\Microsoft\Edge\Application\114.0.1823.43\msedgewebview2.exe

## Resources:

- <https://medium.com/@MalFuzzer/one-electron-to-rule-them-all-dc2e9b263daf>

## Acknowledgements:

- Uriel Kosayev ([@MalFuzzer](#))
- Hai Vaknin ([@VakninHai](#))
- Tamir Yehuda ([@Tamirye94](#))
- Matan Bahar ([@BI4ckShad3](#))

## Detections:

- Sigma: [https://github.com/SigmaHQ/sigma/blob/e1a713d264ac072bb76b5c4e5f41315a015d3f41/rules/windows/process\\_creation/proc\\_creation\\_win\\_susp\\_electron\\_execution\\_proxy.yml](https://github.com/SigmaHQ/sigma/blob/e1a713d264ac072bb76b5c4e5f41315a015d3f41/rules/windows/process_creation/proc_creation_win_susp_electron_execution_proxy.yml)
- IOC: msedgewebview2.exe spawned with any of the following: --gpu-launcher, --utility-cmd-prefix, --renderer-cmd-prefix, --browser-subprocess-path

## Execute

This command launches the Microsoft Edge WebView2 browser control without sandboxing and will spawn calc.exe as its subprocess.

```
msedgewebview2.exe --no-sandbox --browser-subprocess-path="C:\Windows\System32\calc.exe"
```

<b>Use case:</b>	Proxy execution of binary
<b>Privileges required:</b>	Low privileges
<b>Operating systems:</b>	Windows 10, Windows 11
<b>ATT&amp;CK® technique:</b>	T1218.015

This command launches the Microsoft Edge WebView2 browser control without sandboxing and will spawn calc.exe as its subprocess.

```
msedgewebview2.exe --utility-cmd-prefix="calc.exe"
```

<b>Use case:</b>	Proxy execution of binary
------------------	---------------------------

**Privileges required:** User  
**Operating systems:** Windows 10, Windows 11  
**ATT&CK® technique:** T1218.015

. This command launches the Microsoft Edge WebView2 browser control without sandboxing and will spawn calc.exe as its subprocess.

```
msedgewebview2.exe --disable-gpu-sandbox --gpu-launcher="calc.exe"
```

**Use case:** Proxy execution of binary  
**Privileges required:** User  
**Operating systems:** Windows 10, Windows 11  
**ATT&CK® technique:** T1218.015

. This command launches the Microsoft Edge WebView2 browser control without sandboxing and will spawn calc.exe as its subprocess.

```
msedgewebview2.exe --no-sandbox --renderer-cmd-prefix="calc.exe"
```

**Use case:** Proxy execution of binary  
**Privileges required:** User  
**Operating systems:** Windows 10, Windows 11  
**ATT&CK® technique:** T1218.015