

Open in app 

Sign up

Sign in

Medium

 Search

 Write



# T1218.008 — DLL execution using ODBCCONF.exe



Harjot Shah Singh · [Follow](#)



## Medium

Sign up to discover human stories that deepen your understanding of the world.

### Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

### ✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

*Threat actors can abuse ODBCConf.exe in a number of ways, including: Malware Persistence, Data Exfiltration, Credential Theft, Malicious Software Execution, etc.*

*This writing will cover how threat actors can execute malicious DLL using odbccong.exe binary.*

## *Creating a DLL to execute calc.exe?*

Following C++ code can be compiled using Visual Studio as a DLL and upon execution of the compiled DLL, it will execute calc.exe.

# Medium

Sign up to discover human stories that deepen your understanding of the world.

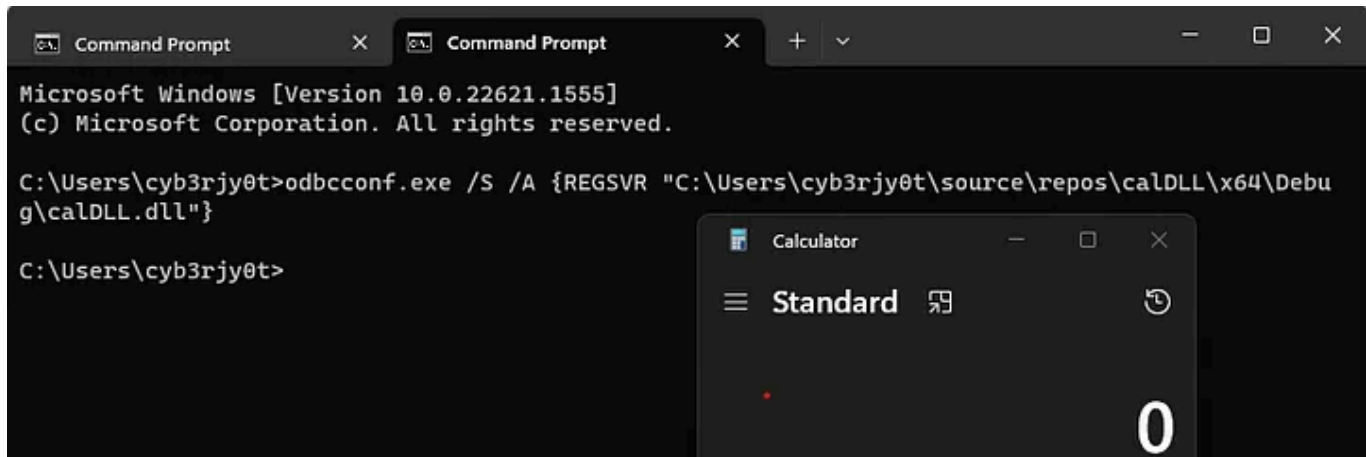
## Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

## ✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Upon execution of the command, following artifacts are generated:



```
Microsoft Windows [Version 10.0.22621.1555]
(c) Microsoft Corporation. All rights reserved.

C:\Users\cyb3rjy0t>odbcconf.exe /S /A {REGSVR "C:\Users\cyb3rjy0t\source\repos\calDLL\x64\Debug\calDLL.dll"}

C:\Users\cyb3rjy0t>
```

## Medium

Sign up to discover human stories that deepen your understanding of the world.

### Free

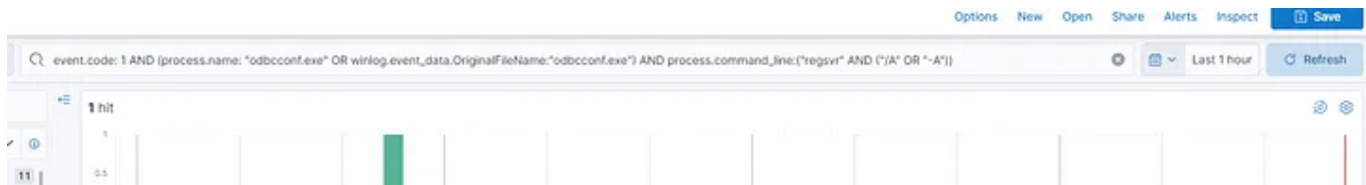
- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

### ✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

## 1. Monitoring the process command line in event ID 1

```
event.code: 1 AND (process.name: "odbcconf.exe" OR original.file_name:"odbcconf.exe"
```



# Medium

Sign up to discover human stories that deepen your understanding of the world.

### Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

### ✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

- <https://attack.mitre.org/techniques/T1218/008/>
- <https://dmcxblue.gitbook.io/red-team-notes-2-0/red-team-techniques/defense-evasion/t1218-signed-binary-proxy-execution/untitled-4>
- <https://learn.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-ver16>
- <https://redcanary.com/blog/raspberry-robin/>
- <https://chat.openai.com/>

## Medium

Sign up to discover human stories that deepen your understanding of the world.

### Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

### ✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

# Medium

Sign up to discover human stories that deepen your understanding of the world.

## Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

## ✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app