https://www.malvuln.com/advisory/7d7ee58c2696794b3be958b165eb61a9.tx


```
Discovery / credits: Malvuln - malvuln.com (c) 2022
Original source: https://malvuln.com/advisory/7d7ee58c2696794b3be958b165eb61a9.txt
Contact: malvuln13@gmail.com
Media: twitter.com/malvuln

Threat: REvil Ransom
Vulnerability: Code Execution
Description: REvil looks for and executes DLLs in its current directory. Therefore, we can potentially hijack
Family: REvil
Type: PE32
MD5: 7d7ee58c2696794b3be958b165eb61a9
Vuln ID: MVID-2022-0577
Disclosure: 05/03/2022
Video PoC URL: https://www.youtube.com/watch?v=WnDxcYzfbUQ

Exploit/PoC:
1) Compile the following C code as "CLDAPI.dll"
2) Place the DLL in same directory as the ransomware
3) Optional - Hide it: attrib +s +h "CLDAPI.dll"
4) Run Conti

#include "windows.h"
#include "stdio.h"

//By malvuln
//Purpose: Code Execution
//Target: REvi Ransomware
//MD5: 7d7ee58c2696794b3be958b165eb61a9
/** DISCLAIMER:
Author is NOT responsible for any damages whatsoever by using this software or improper malware
handling. By using this code you assume and accept all risk implied or otherwise.
**/

//gcc -c CLDAPI.c -m32
//gcc -shared -o CLDAPI.dll CLDAPI.o -m32

BOOL APIENTRY DllMain(HINSTANCE hInst, DWORD reason, LPVOID reserved){
  switch (reason) {
  case DLL_PROCESS_ATTACH:
   MessageBox(NULL, "Code Exec", "by malvuln", MB_OK);
   TCHAR buf[MAX_PATH];
   GetCurrentDirectory(MAX_PATH, TEXT(buf));
   int rc = strcmp("C:\\Windows\\System32", TEXT(buf));
        if(rc != 0){
        HANDLE handle = OpenProcess(PROCESS_TERMINATE, FALSE, getpid());
```

```
     if (NULL != handle) {
        TerminateProcess(handle, 0);
       CloseHandle(handle);
     }
   }
    break;
  }
  return TRUE;
}


Disclaimer: The information contained within this advisory is supplied "as-is" with no warranties or guarante
```
