Diving into Spooler:

Discovering LPE and RCE Vulnerabilities in Windows Printer Driver

Zesen Ye @ Cyber-Kunlun
Dr. Zhiniang Peng @HUST & Cyber-Kunlun

WhoAmI

Zhiniang Peng @edwardzpeng
Associate Professor @HUST
Security Researcher @Cyber-Kunlun

PhD in Cryptography, Work in Defensive & Offensive security

Published many research in both Industry & Academia

More about me:https://sites.google.com/site/zhiniangpeng

HUST : Huazhong University of Science and Technology

Cyber-Kunlun:World-Leading Vulnerability Research in China

Some of My Bugs

CVE-2018-20694,CVE-2018-20746,CVE-2018-20693,CVE-2018-20692,CVE-2018-20696,CVE-2018-20689,CVE-2018-20690,CVE-2018-10812,CVE-2019-6184,CVE-2019-6186,CVE-2019-6487,CVE-2019-1253,CVE-2019-1292,CVE-2019-1317,CVE-2019-1340,CVE-2019-1342,CVE-2019-1374,CVE-2019-8162,CVE-2019-1474,CVE-2019-18371,CVE-2019-18370,CVE-2020-0616,CVE-2020-0635,CVE-2020-0636,CVE-2020-0638,CVE-2020-0641,CVE-2020-0648,CVE-2020-0697,CVE-2020-0730,CVE-2020-3808,CVE-2020-0747,CVE-2020-0753,CVE-2020-0754,CVE-2020-0777,CVE-2020-0780,CVE-2020-0785,CVE-2020-0786,CVE-2020-0789,CVE-2020-0794,CVE-2020-0797,CVE-2020-0800,CVE-2020-0805,CVE-2020-0808,CVE-2020-0819,CVE-2020-0822,CVE-2020-0835,CVE-2020-0841,CVE-2020-0844,CVE-2020-0849,CVE-2020-0854,CVE-2020-0858,CVE-2020-0863,CVE-2020-0864,CVE-2020-0865,CVE-2020-0868,CVE-2020-0871,CVE-2020-0896,CVE-2020-0897,CVE-2020-0899,CVE-2020-0900,CVE-2020-0934,CVE-2020-0935,CVE-2020-0936,CVE-2020-0942,CVE-2020-0944,CVE-2020-0983,CVE-2020-0985,CVE-2020-0989,CVE-2020-1000,CVE-2020-1002,CVE-2020-1010,CVE-2020-1011,CVE-2020-1029,CVE-2020-1068,CVE-2020-1077,CVE-2020-1084,CVE-2020-1086,CVE-2020-1090,CVE-2020-1094,CVE-2020-1109,CVE-2020-1120,CVE-2020-1121,CVE-2020-1123,CVE-2020-1124,CVE-2020-1125,CVE-2020-1131,CVE-2020-1134,CVE-2020-1137,CVE-2020-1139,CVE-2020-1144,CVE-2020-1146,CVE-2020-1151,CVE-2020-1155,CVE-2020-1156,CVE-2020-1157,CVE-2020-1158,CVE-2020-1163,CVE-2020-1164,CVE-2020-1165,CVE-2020-1166,CVE-2020-1184,CVE-2020-1185,CVE-2020-1186,CVE-2020-1187,CVE-2020-1188,CVE-2020-1189,CVE-2020-1190,CVE-2020-1191,CVE-2020-1196,CVE-2020-1199,CVE-2020-1201,CVE-2020-1204,CVE-2020-1209,CVE-2020-1211,CVE-2020-1217,CVE-2020-1222,CVE-2020-1231,CVE-2020-1233,CVE-2020-1235,CVE-2020-1244,CVE-2020-1257,CVE-2020-1264,CVE-2020-1269,CVE-2020-1270,CVE-2020-1273,CVE-2020-1274,CVE-2020-1276,CVE-2020-1277,CVE-2020-1278,CVE-2020-1282,CVE-2020-1283,CVE-2020-1304,CVE-2020-1305,CVE-2020-1306,CVE-2020-1307,CVE-2020-1309,CVE-2020-1312,CVE-2020-1317,CVE-2020-1337,CVE-2020-1344,CVE-2020-1346,CVE-2020-1347,CVE-2020-1352,CVE-2020-1356,CVE-2020-1357,CVE-2020-1360,CVE-2020-1361,CVE-2020-1362,CVE-2020-1364,CVE-2020-5957,CVE-2020-1366,CVE-2020-1372,CVE-2020-1373,CVE-2020-1375,CVE-2020-1385,CVE-2020-1392,CVE-2020-1393,CVE-2020-1394,CVE-2020-1399,CVE-2020-1404,CVE-2020-1405,CVE-2020-1424,CVE-2020-1427,CVE-2020-1441,CVE-2020-0518,CVE-2020-1461,CVE-2020-1465,CVE-2020-1472,CVE-2020-1474,CVE-2020-1475,CVE-2020-1484,CVE-2020-1485,CVE-2020-1511,CVE-2020-1512,CVE-2020-0516,CVE-2020-1516,CVE-2020-1517,CVE-2020-1518,CVE-2020-1519,CVE-2020-1521,CVE-2020-1522,CVE-2020-1524,CVE-2020-1528,CVE-2020-1538,CVE-2020-8741,CVE-2020-1548,CVE-2020-1549,CVE-2020-1550,CVE-2020-1552,CVE-2020-1590,CVE-2020-1130,CVE-2020-16851,CVE-2020-16852,CVE-2020-1122,CVE-2020-1038,CVE-2020-17089,CVE-2020-16853,CVE-2020-16879,CVE-2020-16900,CVE-2020-16980,CVE-2020-17014,CVE-2020-17070,CVE-2020-17073,CVE-2020-17074,CVE-2020-17075,CVE-2020-17076,CVE-2020-17077,CVE-2020-17092,CVE-2020-17097,CVE-2020-17120,CVE-2021-1649,CVE-2021-1650,CVE-2021-1651,CVE-2021-1659,CVE-2021-1680,CVE-2021-1681,CVE-2021-1686,CVE-2021-1687,CVE-2021-1688,CVE-2021-1689,CVE-2021-1690,CVE-2021-1718,CVE-2021-1722,CVE-2021-24072,CVE-2021-24077,CVE-2021-3750,CVE-2021-24088,CVE-2021-26869,CVE-2021-26870,CVE-2021-26871,CVE-2021-26885,CVE-2021-28347,CVE-2021-28351,CVE-2021-28436,CVE-2021-28450,CVE-2021-31966,CVE-2021-34527,CVE-2021-42321,CVE-2021-36970,CVE-2021-38657,CVE-2021-40485,CVE-2021-41366,CVE-2021-42294,CVE-2021-42297,CVE-2021-43216,CVE-2021-43223,CVE-2021-43248,CVE-2022-21835,CVE-2022-21837,CVE-2022-21878,CVE-2022-21881,CVE-2022-21888,CVE-2022-21971,CVE-2022-21974,CVE-2022-21992,CVE-2022-23285,CVE-2022-23290,CVE-2022-24454,CVE-2022-29108,CVE-2022-24547,CVE-2022-23270,CVE-2022-26930,CVE-2022-29103,CVE-2022-29113,CVE-2022-38036,CVE-2022-35793,CVE-2022-35755,CVE-2022-35749,CVE-2022-35746,CVE-2022-34690,CVE-2022-21980,CVE-2022-22050,CVE-2022-22024,CVE-2022-22022,CVE-2022-30226,CVE-2022-30157,CVE-2022-29108,CVE-2022-21999,CVE-2023-21683,CVE-2023-21684,CVE-2023-21693,CVE-2023-21801,CVE-2023-23403,CVE-2023-23406,CVE-2023-23413,CVE-2023-24856,CVE-2023-24857,CVE-2023-24858,CVE-2023-24863,CVE-2023-24865,CVE-2023-24866,CVE-2023-24867,CVE-2023-24907,CVE-2023-24868,CVE-2023-24909,CVE-2023-24870,CVE-2023-24872,CVE-2023-24913,CVE-2023-24876,CVE-2023-24924,CVE-2023-24883,CVE-2023-24925,CVE-2023-24884,CVE-2023-24926,CVE-2023-24885,CVE-2023-24927,CVE-2023-24886,CVE-2023-24928,CVE-2023-24887,CVE-2023-24929,CVE-2023-28243,CVE-2023-28296,CVE-2023-29366,CVE-2023-29367,CVE-2023-32017,CVE-2023-32039,CVE-2023-32040,CVE-2023-32041,CVE-2023-32042,CVE-2023-32085,CVE-2023-35296,CVE-2023-35302,CVE-2023-35306,CVE-2023-35313,CVE-2023-35323,CVE-2023-35324,CVE-2023-36898,CVE-2023-36792,CVE-2023-36704,CVE-2023-36418,CVE-2023-36395,CVE-2023-36393,CVE-2023-35624,CVE-2023-21683,CVE-2023-29366,CVE-2023-46138,CVE-2023-42820,CVE-2023-42819,CVE-2024-21426,CVE-2024-29156,CVE-2024-26198,CVE-2024-21435,CVE-2024-21329,CVE-2024-21384,CVE-2024-20691,CVE-2024-21433,CVE-2024-20694,CVE-2024-0087,CVE-2024-0088,CVE-2024-30060,CVE-2024-29989,CVE-2024-38077,CVE-2024-38024,CVE-2024-38023,CVE-2024-38076,CVE-2024-38074,CVE-2024-38073,CVE-2024-35261,CVE-2024-38072,CVE-2024-38071,CVE-2024-38015,CVE-2024-43467,CVE-2024-43455,CVE-2024-38231,CVE-2024-38258,CVE-2024-43454,CVE-2024-38263,CVE-2024-38260,CVE-2024-38228,CVE-2024-43495,CVE-2024-43470,CVE-2024-38225, CVE-2024-43467,CVE-2024-38097,CVE-2024-38262,CVE-2024-43583

WhoAmI

Zesen Ye

Security Researcher @Cyber-Kunlun

Focus on Fuzzing & Windows Applications

MSRC MVR in 2022 ~ 2024

Cyber-Kunlun:World-Leading Vulnerability Research

The largest vulnerability research lab in China

Mission: To secure the digital world through cutting-edge vulnerability insights

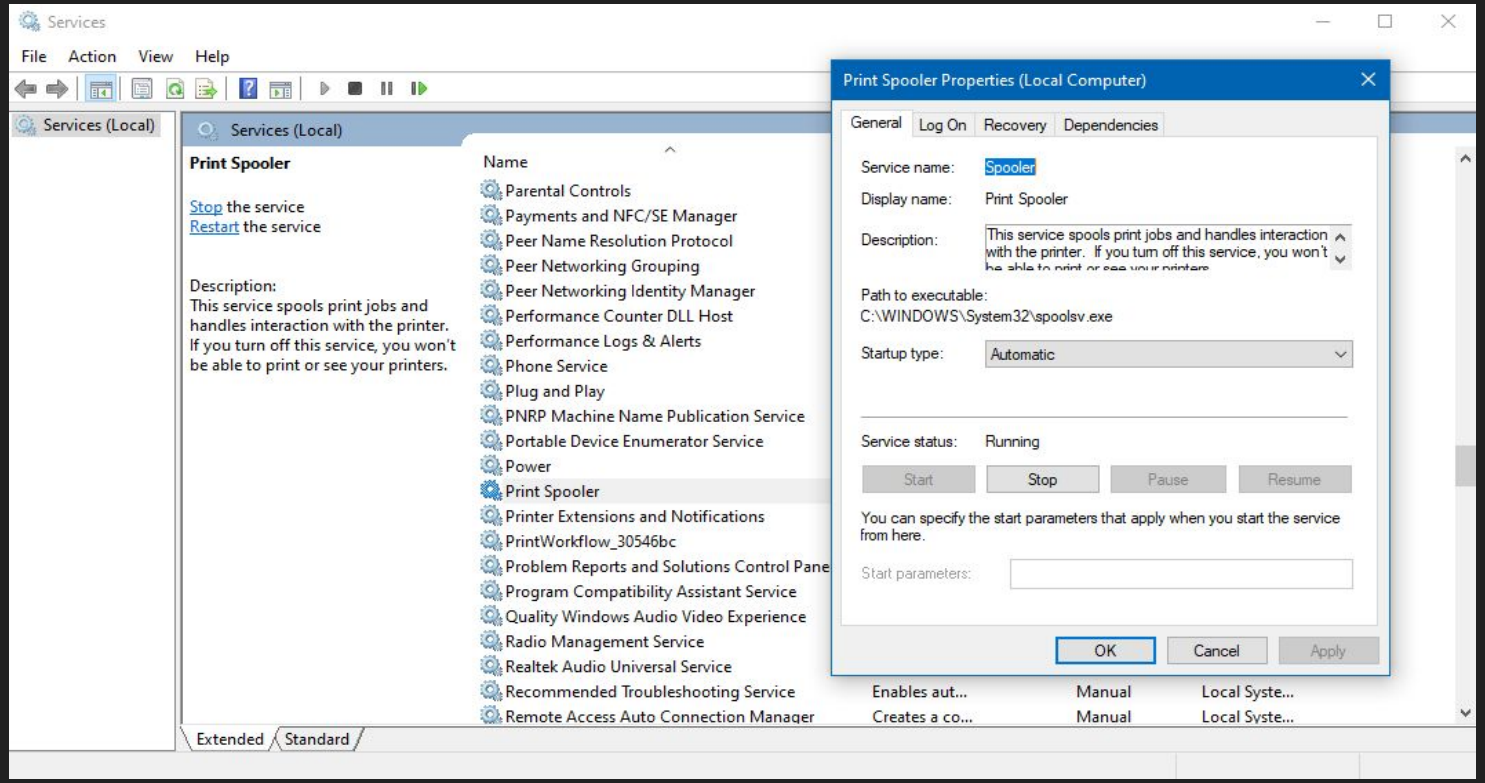
Agenda

1. Introduction
2. New Attack Surface – Windows Printer Driver Rendering
3. Dive into the XPS Format
4. Vulnerability in Resource Parsing
5. Vulnerability in XML Parsing
6. Vulnerability in Third-Party Driver
7. Summary

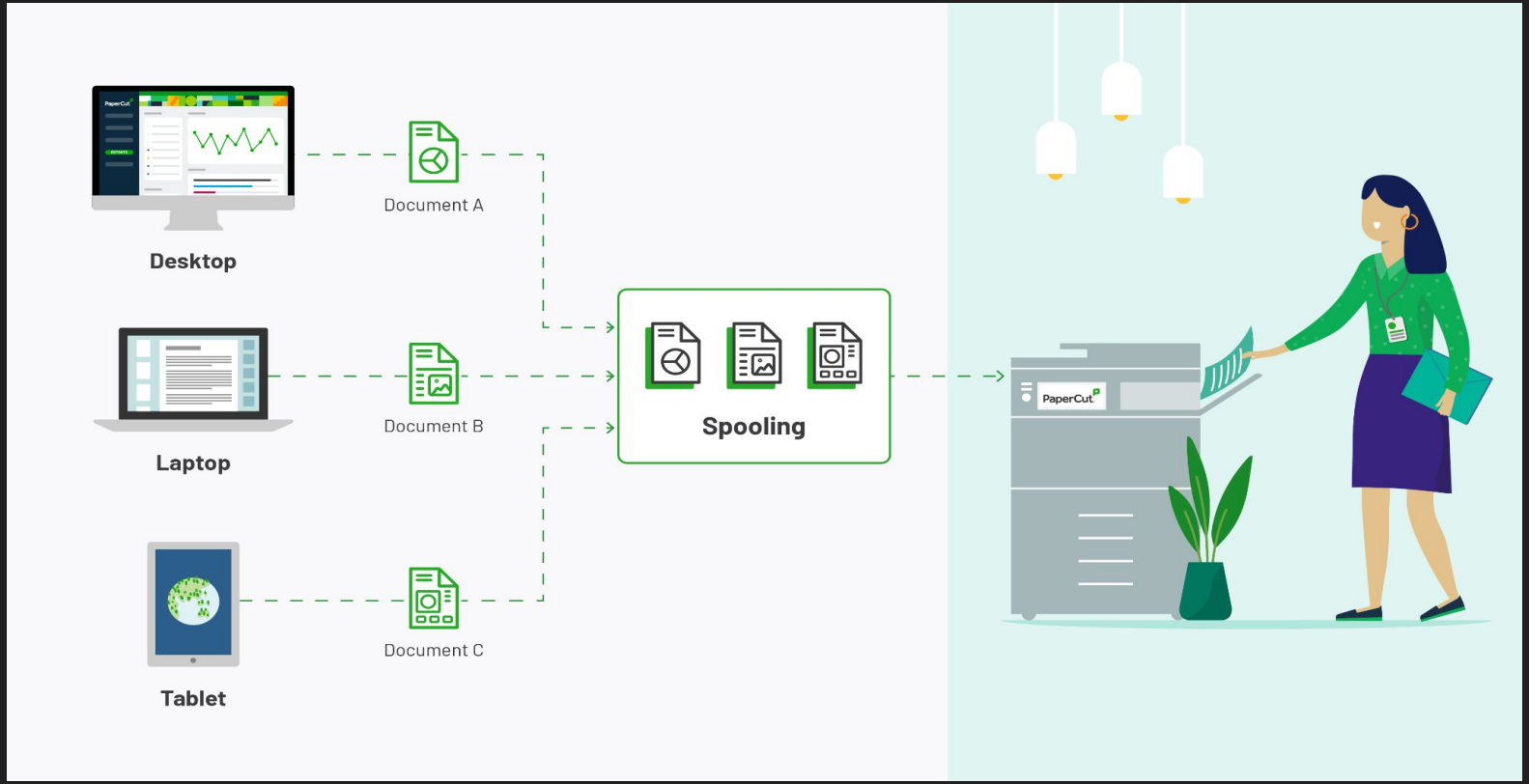
Introduction

Print Spooler

A Windows Service Spools print jobs

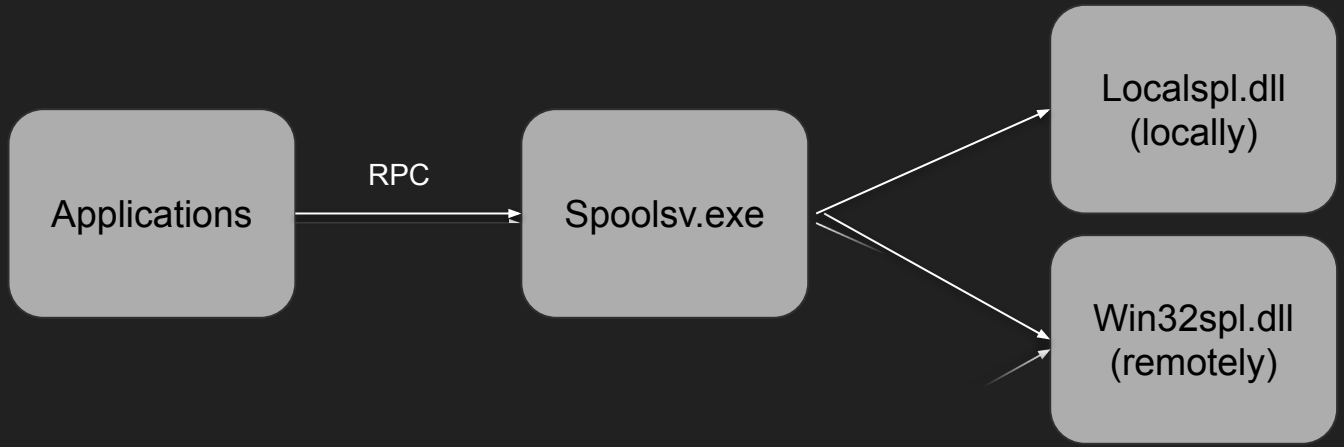


Spooling


Desktop
Document A
Laptop
Document B
Tablet
Document C
Spooling
PaperCut

Printer Spooler

Add, remove and configure printer
Spool high-level function calls into printer jobs
Receive and schedule printer jobs for printing



Previous research

Evil Printer: How To Hack Windows Machines With Printing Protocol - Zhipeng Huo and Chuanda Ding

A Decade After Stuxnet's Printer Vulnerability: Printing is Still the Stairway to Heaven - PELEG HADAR and TOMER BAR

Diving in to Spooler: Discovering LPE and RCE Vulnerabilities in Windows Printer - Zhiniang Peng, Xuefeng Li and Lewis Lee

Windows Security Research: A Practical Guide for Beginners to find 0 days - Oliver Lyak

Print Spooler is hot in Cyber Security

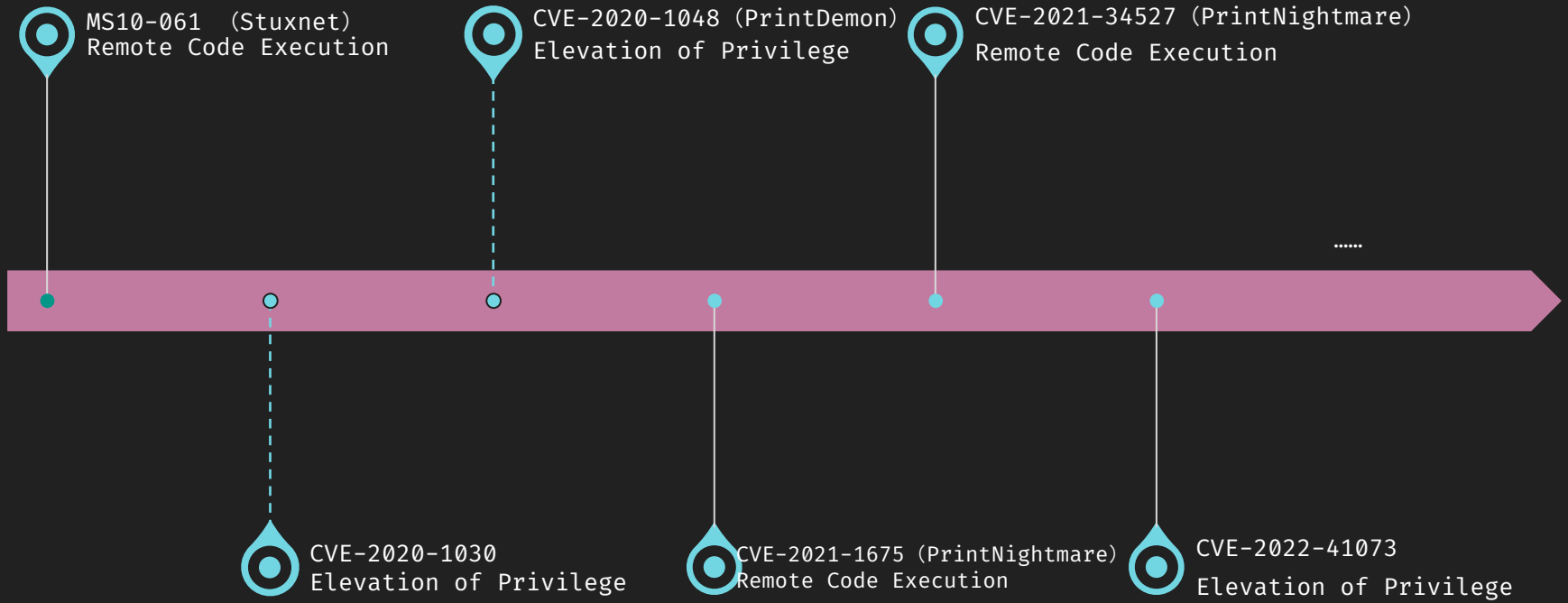
1. The Spooler used to run with high privileges and load code from the network which is prone to security issues

2. Print bugs account for 9% of all Windows cases reported to Microsft according to MSRC blog.

3. A lot Exploited vuls in Spooler in the pasts years

4. Stuxnet, PrintNightmare ……

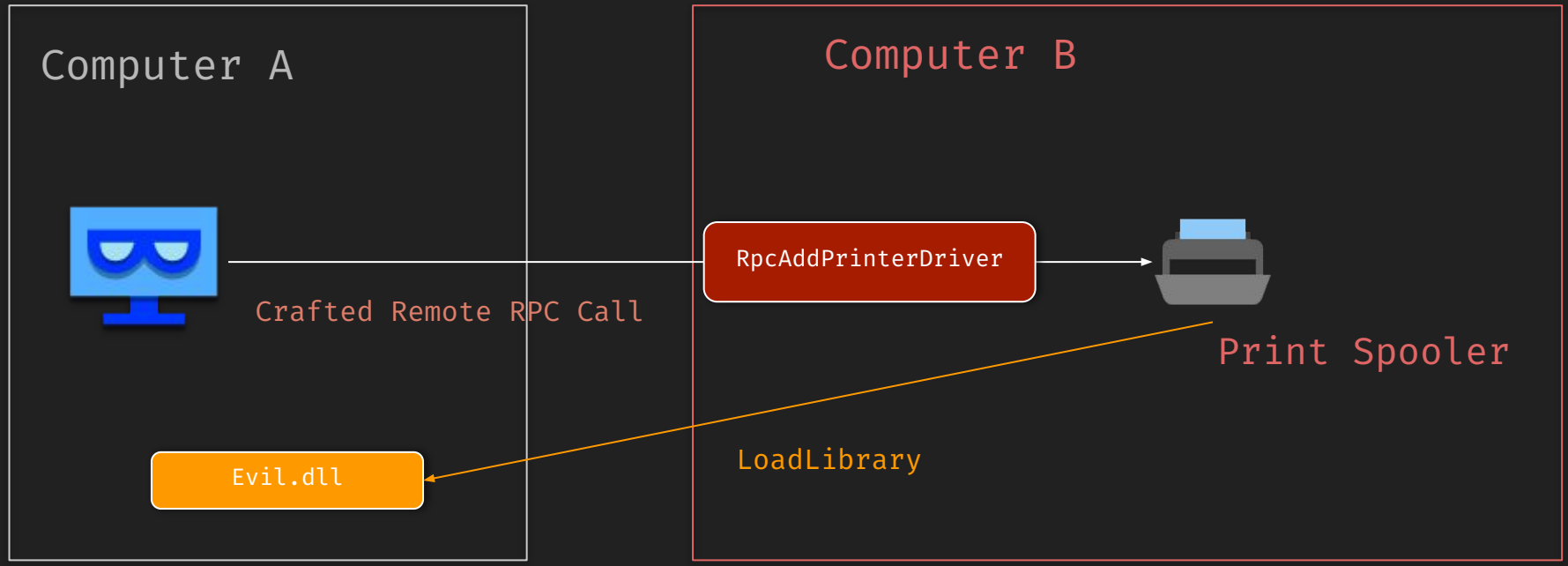
Exploited vuls in the pasts years



Spooler Vulnerability Types

- Path Redirection Attacks(Symbol Link):
  - Exmaple:CVE-2020-1048, ...
- Path Traversal:
  - Exmaple:CVE-2020-1300, ...
- Arbitrary Dll Loading:
  - Exmaple:PrintNightmare, ...
- Memory Corruption:
  - Exmaple:CVE-2021-24077, …
- …

PrintNightmare

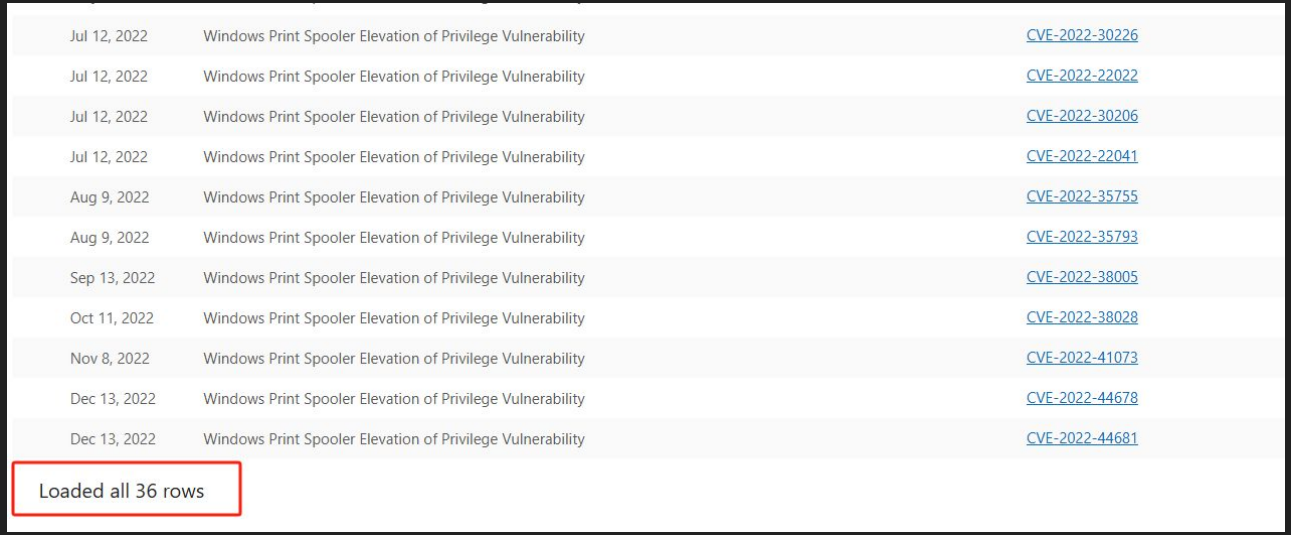


More story about PrintNightmare:
Diving in to Spooler: Discovering LPE and RCE Vulnerabilities in Windows Printer
Zhiniang Peng, Xuefeng Li and Lewis Lee

After PrintNightmare

In 2022, Microsoft fixed 36 vulnerabilities for Print Spooler.

Microsft’s fix Broken Print Spooler for many times.



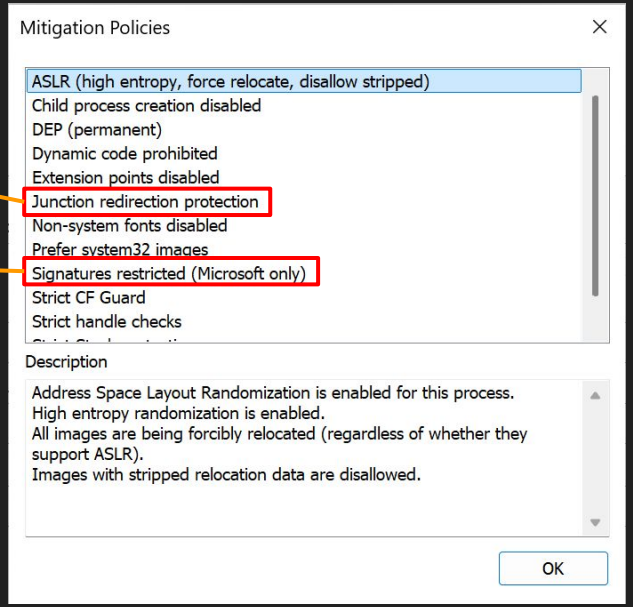
Jul 12, 2022	Windows Print Spooler Elevation of Privilege Vulnerability	CVE-2022-30226
Jul 12, 2022	Windows Print Spooler Elevation of Privilege Vulnerability	CVE-2022-22022
Jul 12, 2022	Windows Print Spooler Elevation of Privilege Vulnerability	CVE-2022-30206
Jul 12, 2022	Windows Print Spooler Elevation of Privilege Vulnerability	CVE-2022-22041
Aug 9, 2022	Windows Print Spooler Elevation of Privilege Vulnerability	CVE-2022-35755
Aug 9, 2022	Windows Print Spooler Elevation of Privilege Vulnerability	CVE-2022-35793
Sep 13, 2022	Windows Print Spooler Elevation of Privilege Vulnerability	CVE-2022-38005
Oct 11, 2022	Windows Print Spooler Elevation of Privilege Vulnerability	CVE-2022-38028
Nov 8, 2022	Windows Print Spooler Elevation of Privilege Vulnerability	CVE-2022-41073
Dec 13, 2022	Windows Print Spooler Elevation of Privilege Vulnerability	CVE-2022-44678
Dec 13, 2022	Windows Print Spooler Elevation of Privilege Vulnerability	CVE-2022-44681

Loaded all 36 rows

Mitigation after PrintNightmare

Block path redirection attacks

Block arbitrary DLL Loading



Is Spooler secure after all the fix?

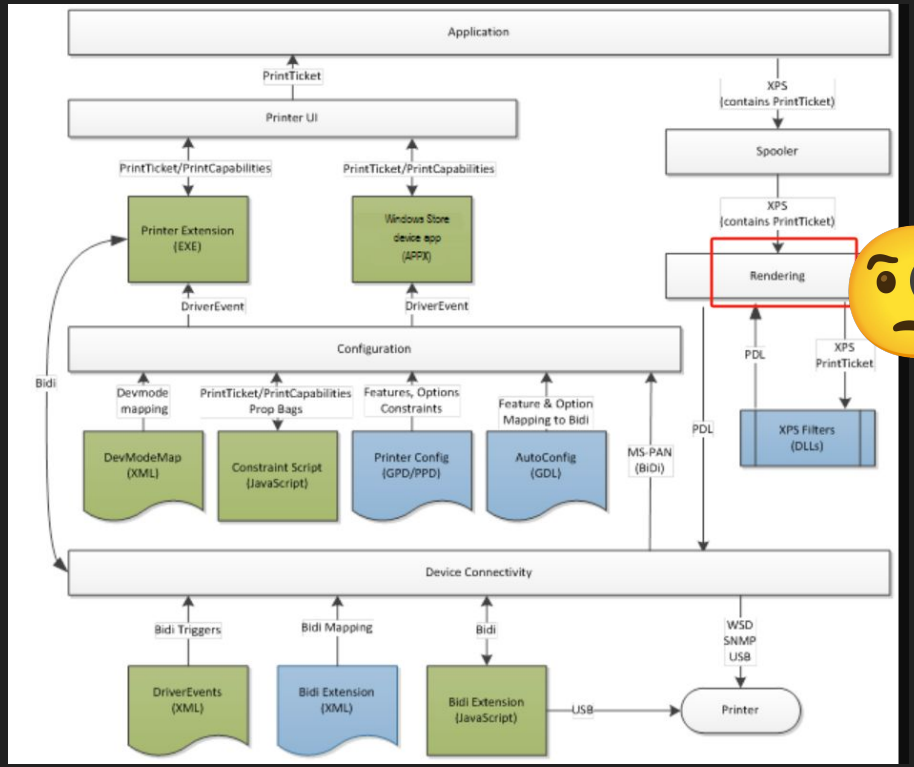
Let’s dive into Spooler,Again!

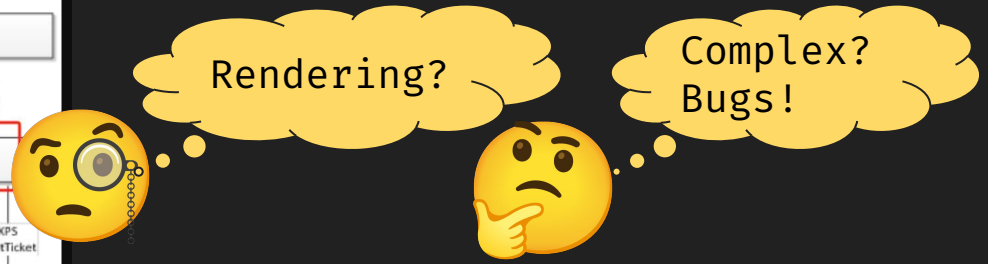
The New Attack Surface

Windows Printer Driver Rendering

New attack surface

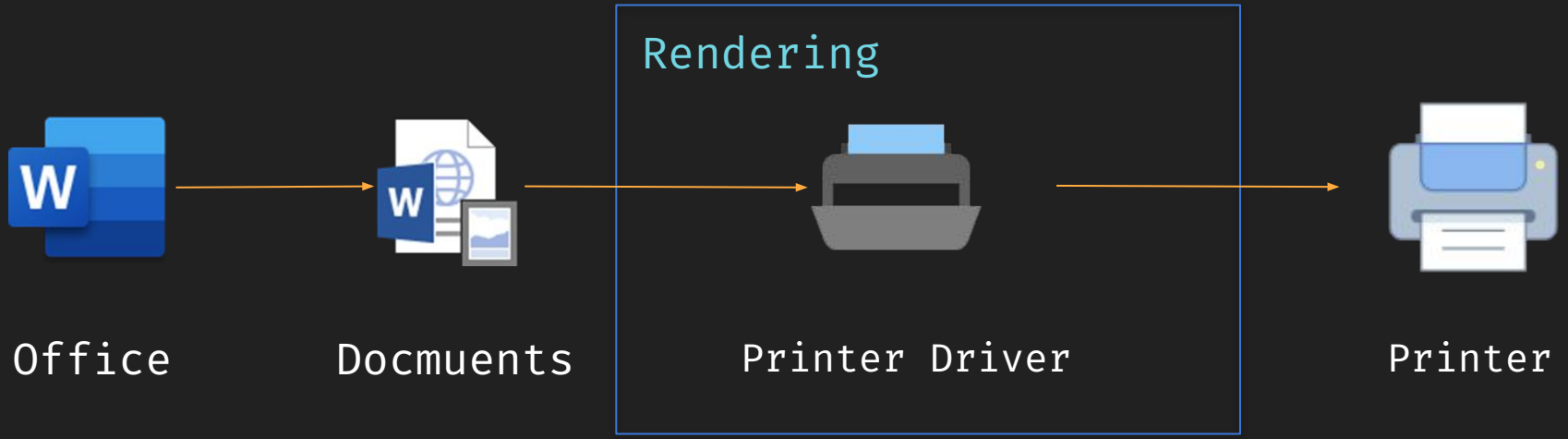
Review the Architecture from MSDN



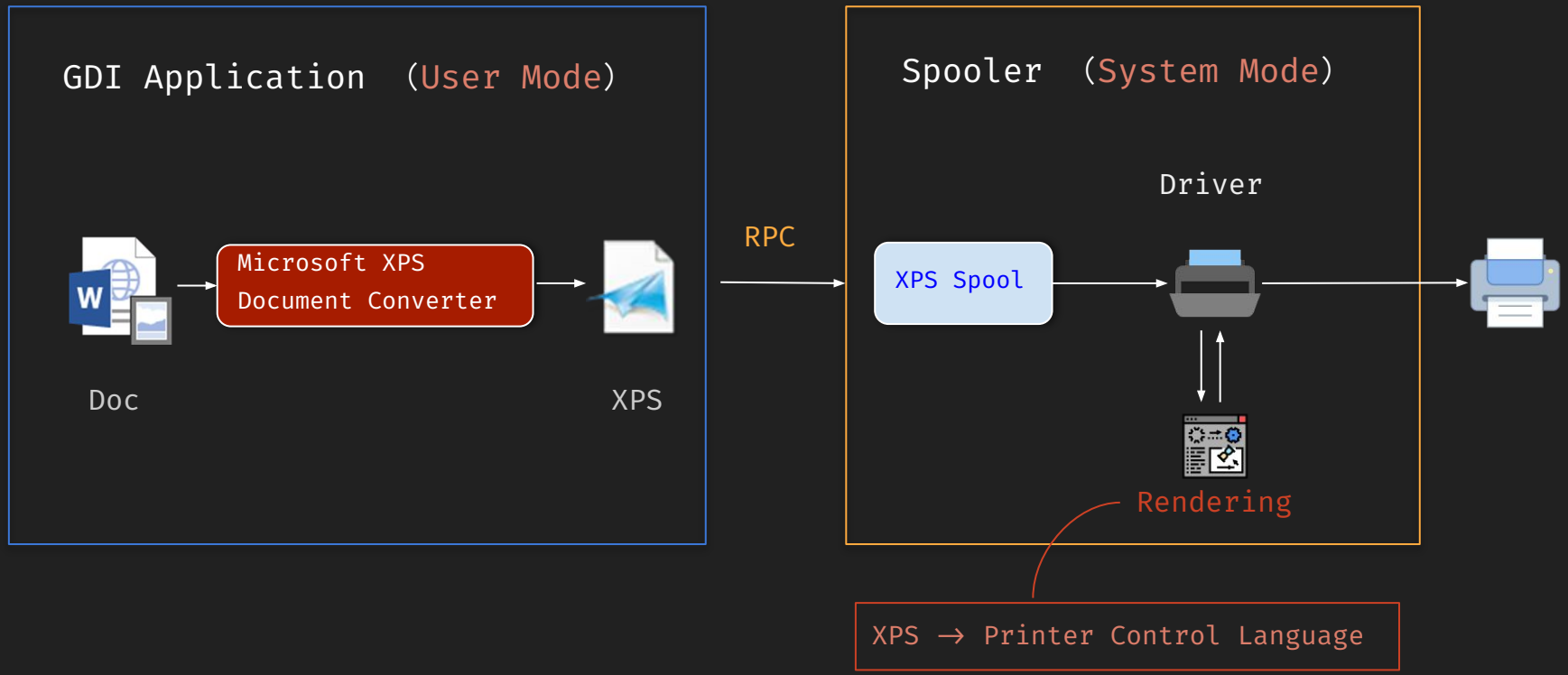


Print example

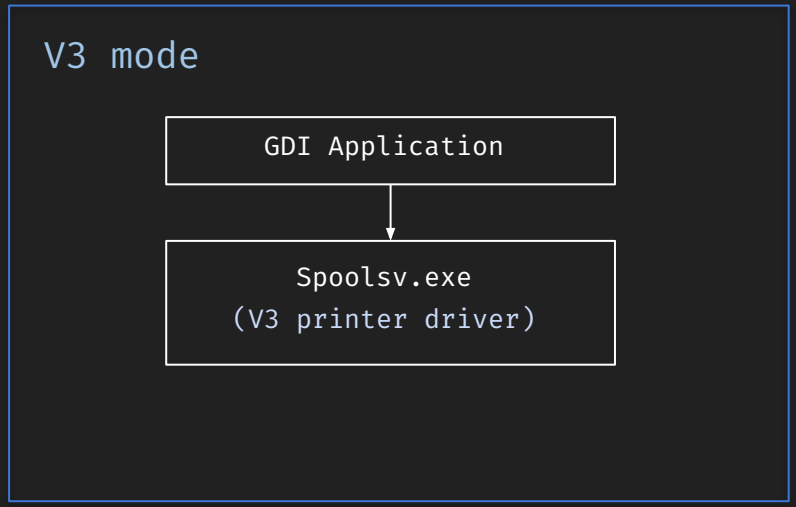
Let’s print a document

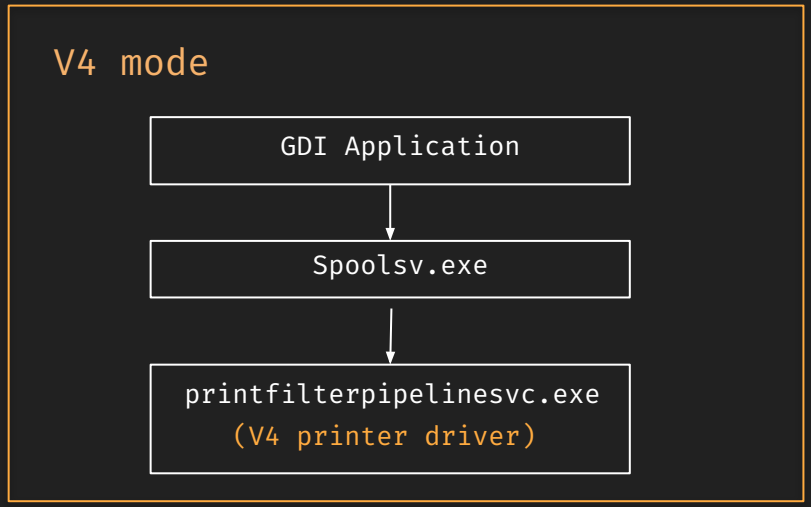


Details


GDI Application (User Mode)
Microsoft XPS Document Converter
Doc
XPS
RPC
Spooler (System Mode)
Driver
XPS Spool
Rendering
XPS → Printer Control Language

V3 print driver & V4 print driver





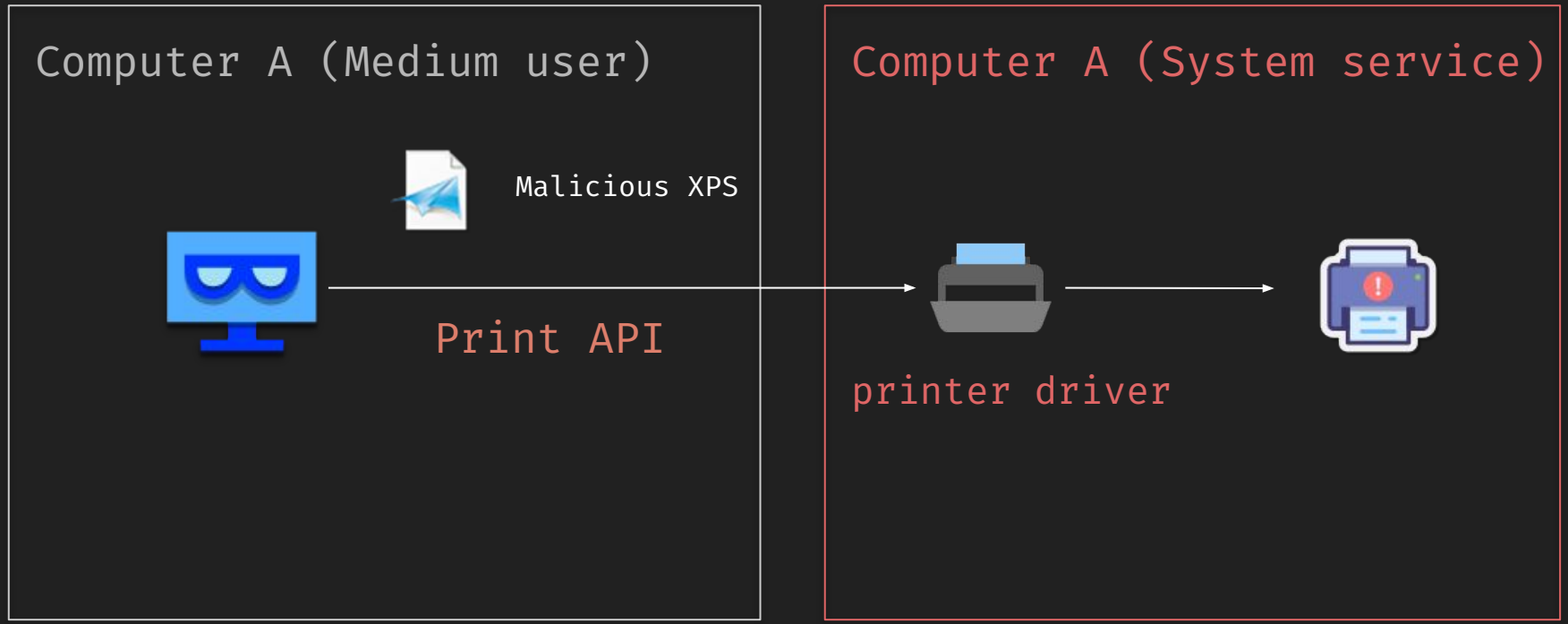
V3 mode : a crash in rendering will DOS entire spooler service.

V4 mode : a crash in rendering will restart printfilterpipelinesvc.exe

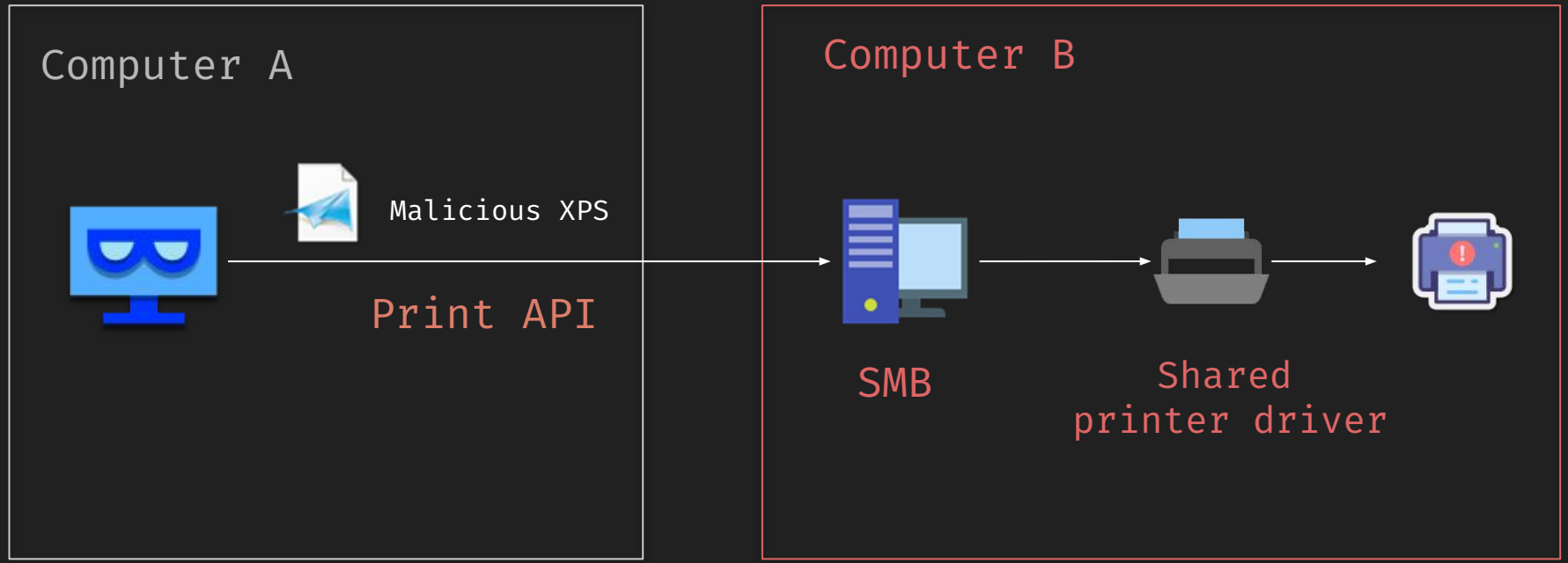
Q: What Rendering Issue Impacts? 

A: LPE & RCE

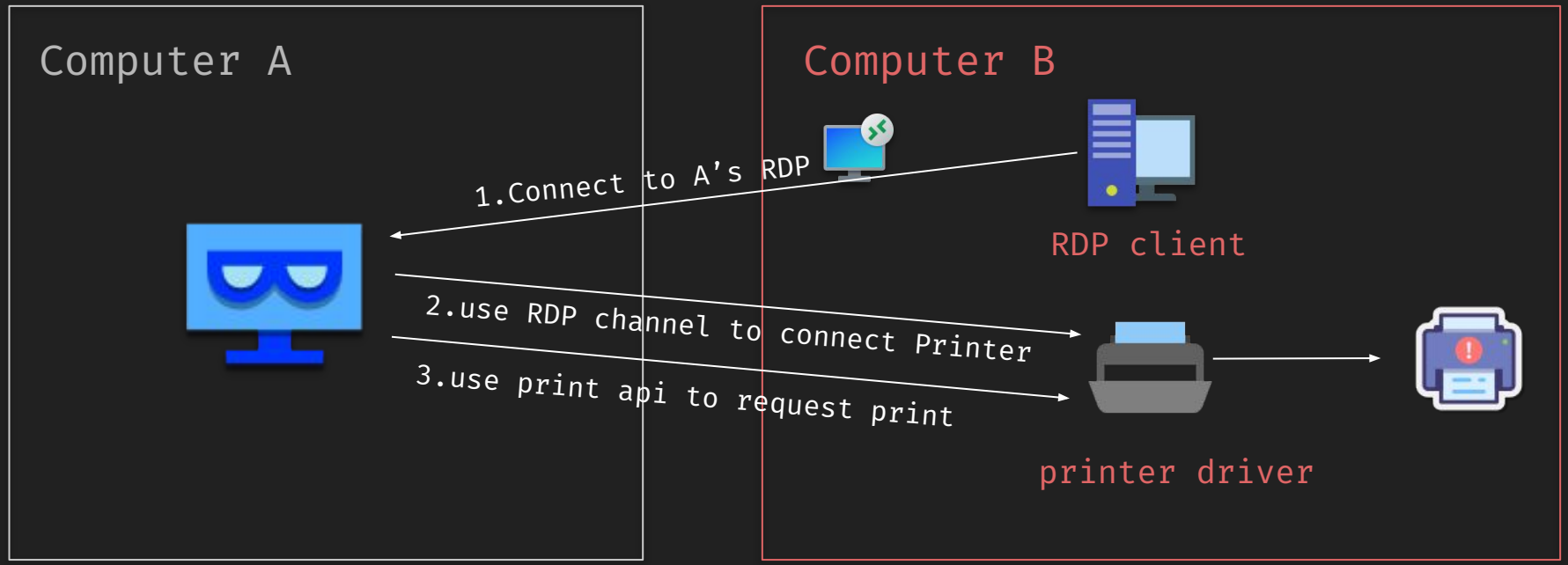
LPE Attack Scenario (Medium2System)



RCE Attack Scenario (RCE over SMB)

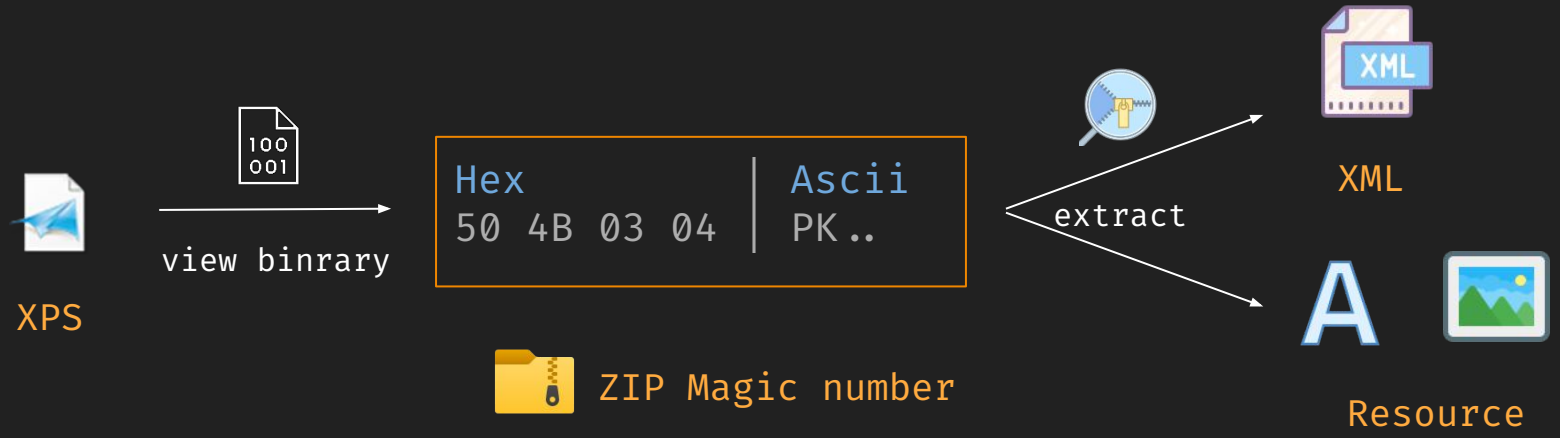


RCE Attack Scenario (RCE over RDP)



Dive into the XPS Format

Open XML Paper Specification



Open XML Paper Specification

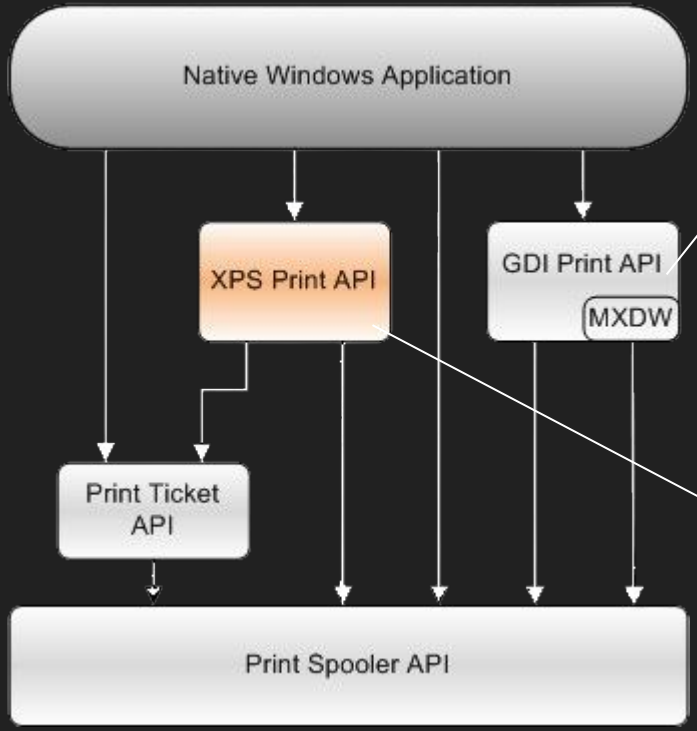
```
<Path>
        <Path.Fill>
                <SolidColorBrush Color="#0000FF" />
         </Path.Fill>
        <Path.Data>
                <PathGeometry>
                        <PathFigure StartPoint="10,10" IsClosed="true">
                                <PolyLineSegment Points="50,200 100,40 150,200
                                        200,10 100,105" />
                        </PathFigure>
                </PathGeometry>
        </Path.Data>
</Path>
```

content

1.fpage

render

How to print



GDI Print API

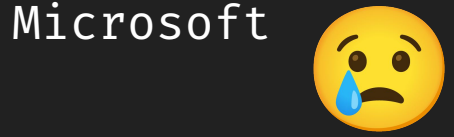
.docx / .pdf / .html → .xps → spooler

XPS Print API

.xps → spooler

How to use XPS Print API

XPS Viewer, but it was deprecated by Microsoft



XPS Viewer	We're changing the way you get XPS Viewer. In Windows 10, version 1709 and earlier versions, the app is included in the installation image. If you have XPS Viewer and you update to Windows 10, version 1803, there's no action required. You'll still have XPS Viewer. However, if you install Windows 10, version 1803, on a new device (or as a clean installation), you can install XPS Viewer from **Apps and Features** in the Settings app or through Features on Demand. If you had XPS Viewer in Windows 10, version 1709, but manually removed it before updating, you'll need to manually reinstall it.	1803

How to use XPS Print API

Make our Application as the harness:

```
HRESULT StartXpsPrintJob(
  [in]  LPCWSTR            printerName,
  [in]  LPCWSTR            jobName,
  [in]  LPCWSTR            outputFileName,
  [in]  HANDLE             progressEvent,
  [in]  HANDLE             completionEvent,
  [in]  UINT8              *printablePagesOn,
  [in]  UINT32             printablePagesOnCount,
  [out] IXpsPrintJob       **xpsPrintJob,
  [out] IXpsPrintJobStream **documentStream,
  [out] IXpsPrintJobStream **printTicketStream
);
```

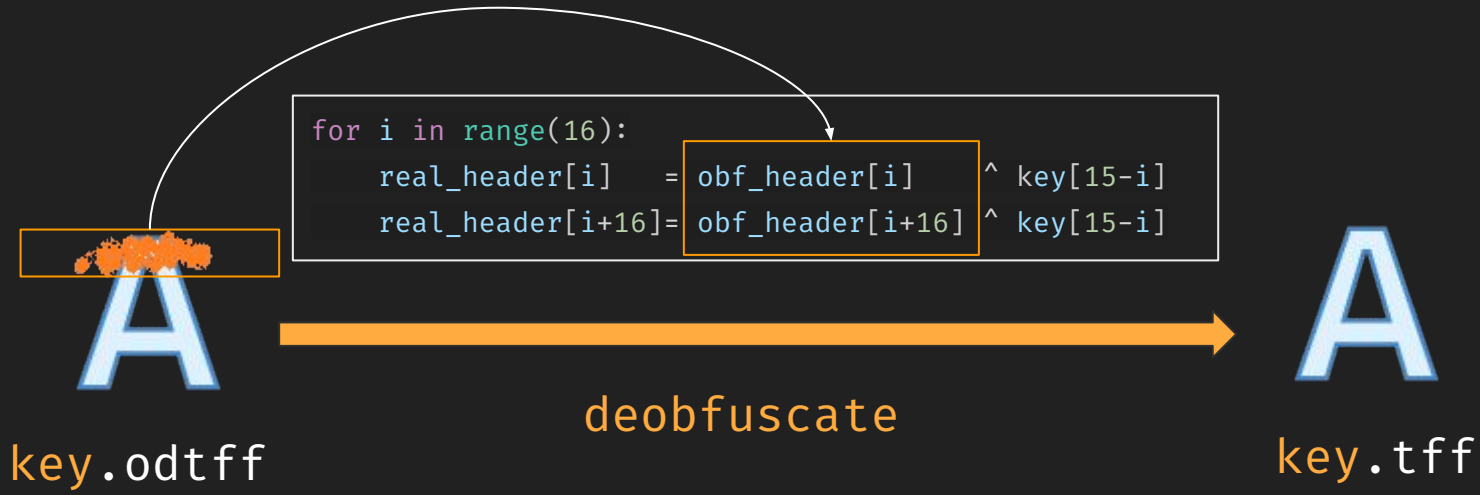
Local: Microsoft PS Class Driver
Remote: \\smb\Microsoft PS Class Driver

IStream::Read(XPS file stream)

Vulnerability in Resource Parsing

ODTTF (Obfuscated OpenType Font)

XPS supports the use of custom embedded fonts to promote diversity, but obfuscation is required



Font

Many researches on fonts before, so we won't dive into the structure of fonts here

We primarily referred to "One font vulnerability to rule them all #1: Introducing the BLEND vulnerability." Posted by Mateusz Jurczyk of Google Project Zero

CVEs in Parsing Font

Microsoft Printer Driver Remote Code Execution Vulnerability

CVE-2023-21684 CVE-2023-21801

CVE-2023-23403 CVE-2023-24876

Microsoft Printer Driver Information Disclosure Vulnerability

CVE-2023-21693 CVE-2023-24857 CVE-2023-24858

CVE-2023-24865 CVE-2023-24866

Case 1

CVE-2023-24863 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability

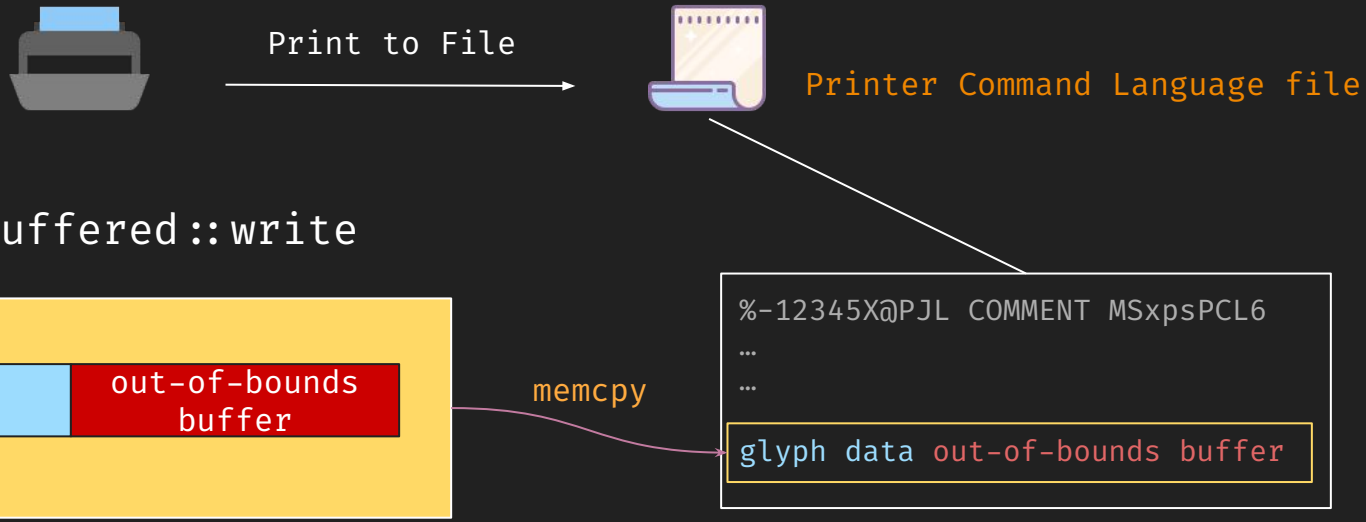
It is an out-of-bounds-read vulnerability in TrueType Parsing

The offset was not checked during the parsing of the glyf table

The unique point here is the crash call stack:

1. msvcrt!memcpy+0×92
2. MSxpsPCL6!cmnStreamBuffered::write+0×85

Case 1



Information Leak!

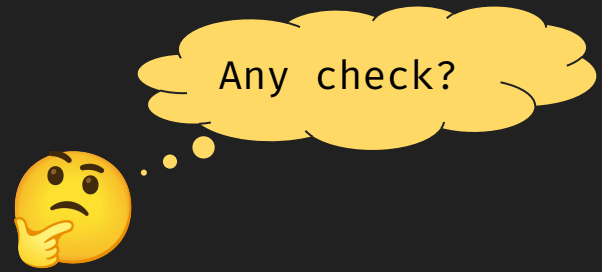
Case 2

CVE-2023-23403 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability

It is an out-of-bounds-write vulnerability in OpenType Parsing

The CFF table contains a Compact Font Format (CFF) font representation and is structured according to Adobe Technical Note #5176: “The Compact Font Format Specification

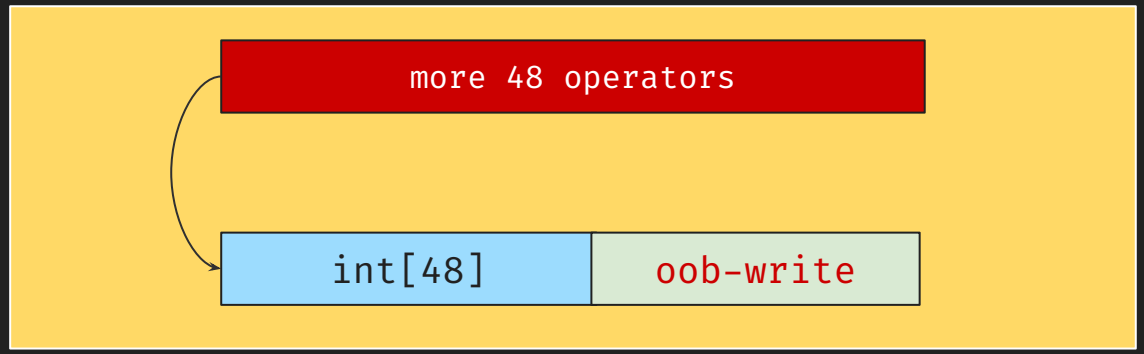
Operators and operands may be distinguished by inspection of their first byte: 0–21 specify operators and 28, 29, 30, and 32–254 specify operands (numbers). Byte values 22–27, 31, and 255 are reserved. An operator may be preceded by up to a maximum of 48 operands.



Case 2

After testing, we found here had no check


```
MSxpsPCL6!cmnCFF::cmnCFF+0×6da:
mov     qword ptr [rax+rcx*8],r9 ds:00000282`9383e000=????????????????
```



Color Management

Color management is supported in v4 print drivers

Common resources file is ICC Profile

International Color Consortium (ICC) color profiles

Provide a cross-platform device profile format

ICC Profile in XPS format

```
<Path>
        <Path.Fill>
                <SolidColorBrush Color="ContextColor /Resources/test.icc
                        1.0,1.000,0.000,0.000,0.000" />
         </Path.Fill>
        <Path.Data>
                <PathGeometry>
                        <PathFigure StartPoint="10,10" IsClosed="true">
                                <PolyLineSegment Points="50,200 100,40 150,200
                                        200,10 100,105" />
                        </PathFigure>
                </PathGeometry>
        </Path.Data>
</Path>
```

content

1.fpage

render

ICC Profile

According to Specification ICC.1:2004-10 (Profile version 4.2.0.0)

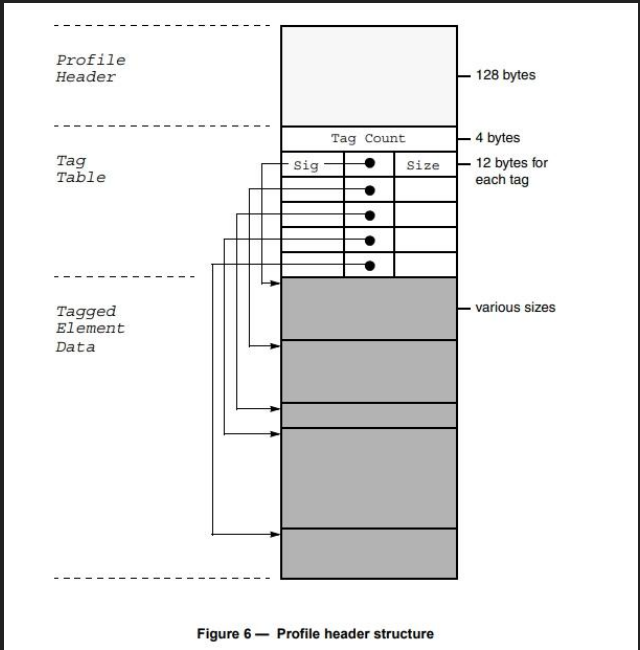


Figure 6 — Profile header structure

😀 Similar as Font

🤔 limited public information available

Requires more time for document reading and reverse engineering

Method to Find Vulnerability

How to find vulnerabilities without reading the document

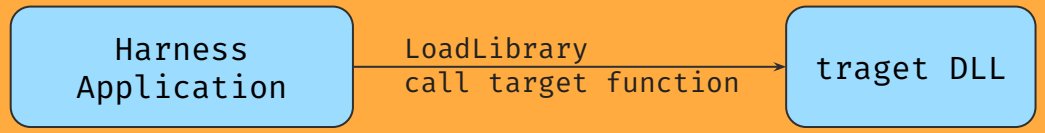
Fuzzing

Choose the Suitable Fuzzing Architecture

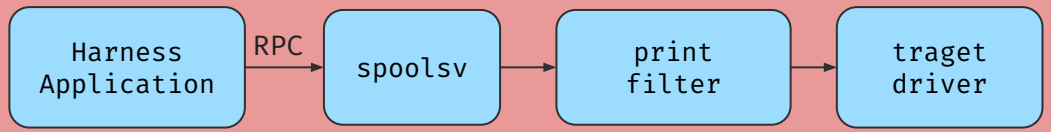
WinAFL @ Ivan Fratric

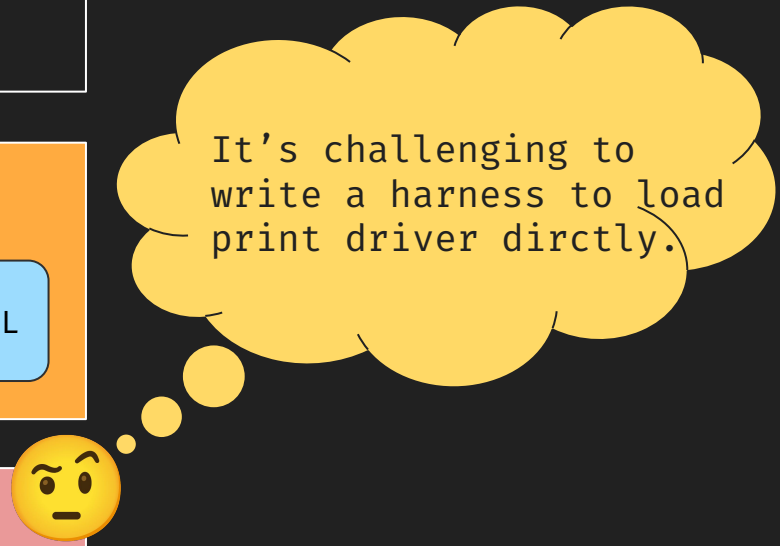
- Most Common Windows Platform Fuzzing
- Our attempts have not been satisfactory

Ideal Scenario for WinAFL



The Scenario of printer drvier rendering

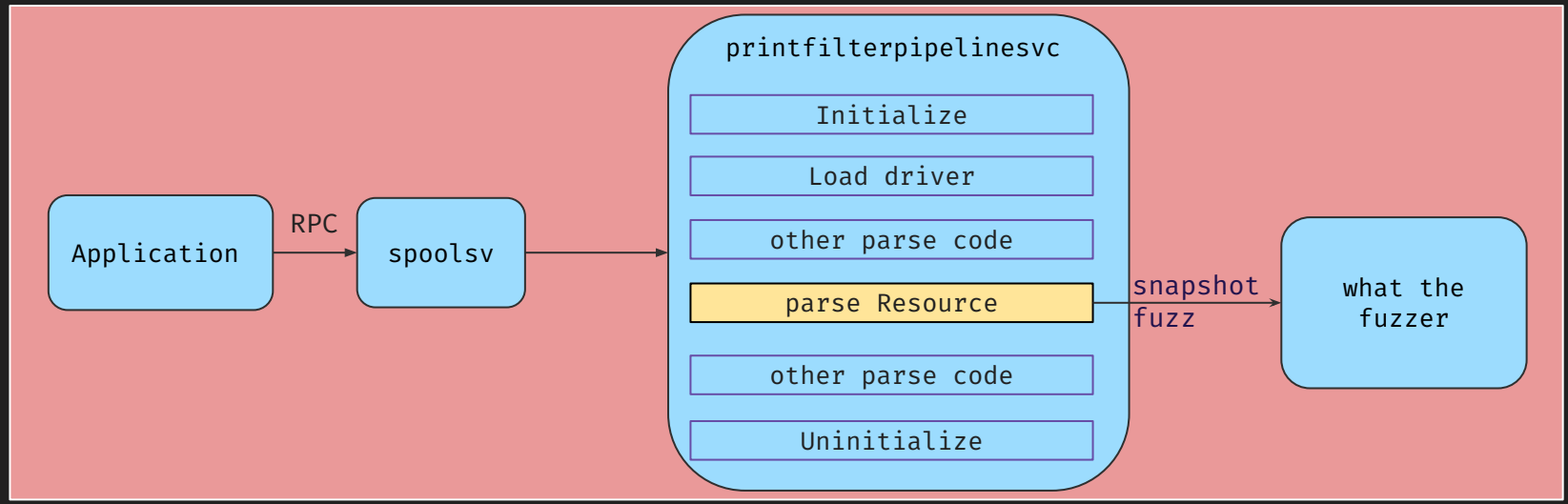




Choose the Suitable Fuzzing Architecture

What the fuzz @ 0vercl0k

A distributed, code-coverage guided, customizable, cross-platform snapshot-based fuzzer designed for attacking user and / or kernel-mode targets running on Microsoft Windows



CVEs in ICC Parsing

Microsoft Printer Driver Remote Code Execution Vulnerability

CVE-2023-23413 CVE-2023-23406

CVE-2023-24867 CVE-2023-24868

CVE-2023-24872 CVE-2023-24907

CVE-2023-24909 CVE-2023-24913

Microsoft Printer Driver Information Disclosure Vulnerability

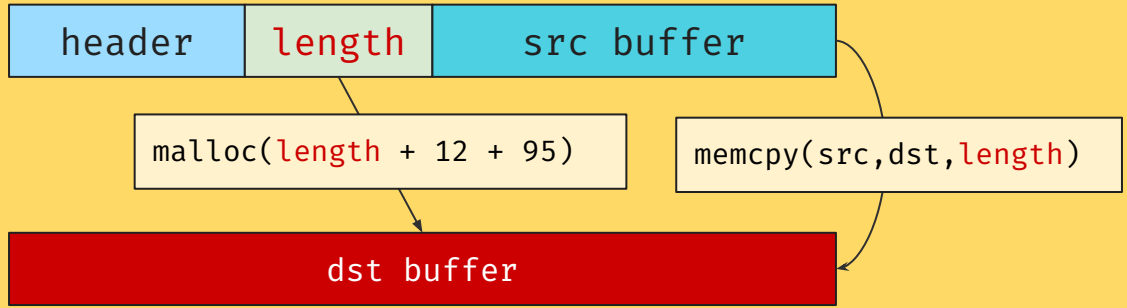
CVE-2023-24870

Case 3

CVE-2023-24909 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability

Weakness: CWE-190: Integer Overflow or Wraparound

profileDescriptionTag




```
if length > len(src)
    Out-of-bounds read

if length = 0×ffffffff
    Integer Overflow
    Out-of-bounds write
```

Vulnerability in XML Parsing

What XML do in XPS?

```
<Path>
        <Path.Fill>
                <SolidColorBrush Color="#0000FF" />
         </Path.Fill>
        <Path.Data>
                <PathGeometry>
                        <PathFigure StartPoint="10,10" IsClosed="true">
                                <PolyLineSegment Points="50,200 100,40 150,200
                                        200,10 100,105" />
                        </PathFigure>
                </PathGeometry>
        </Path.Data>
</Path>
```

content

1.fpage

render

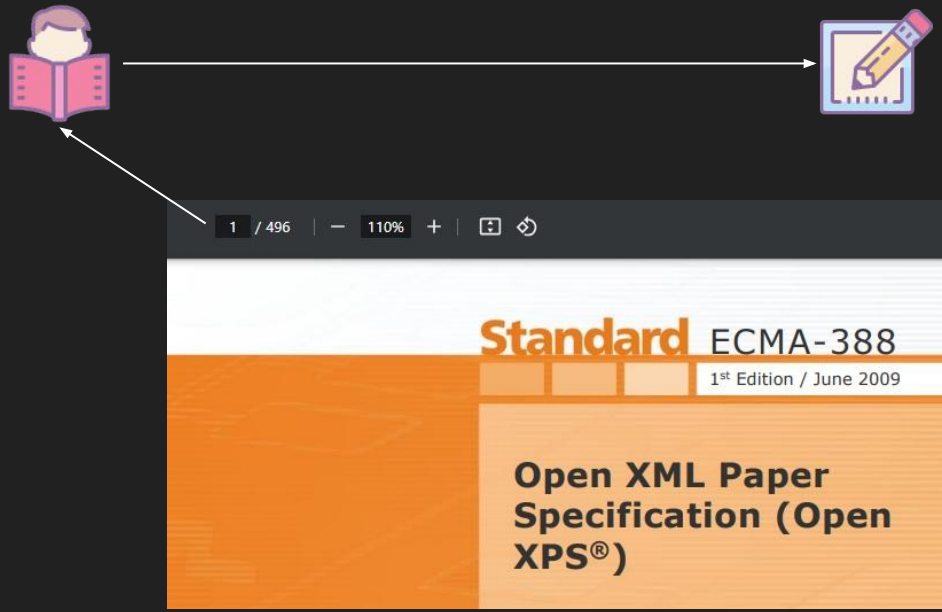
Resources vs XML

- Binary file
  - hard to read
  - easy to mutate
- Resources file possess high versatility
  - easy to collect corpus

- Text file
  - easy to read
  - hard to mutate
- XML formats are designed specifically for software
- Direct use of XPS files is not widespread.
  - hard to collect corpus

How to generate XML

Read 496-page document and create

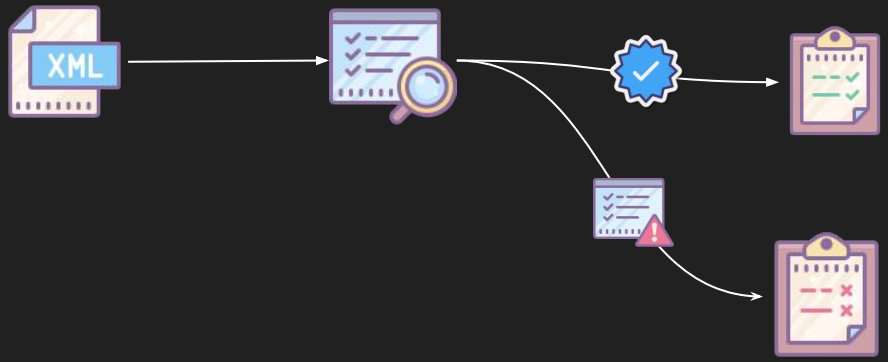


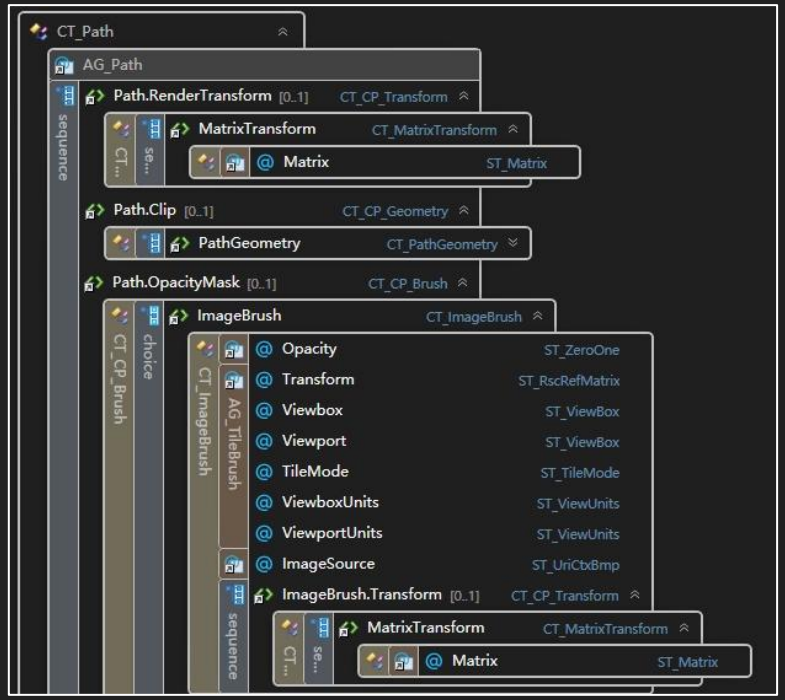
How to generate XML

PrintXPS – Input Generation

XSD – XML Schema Definition

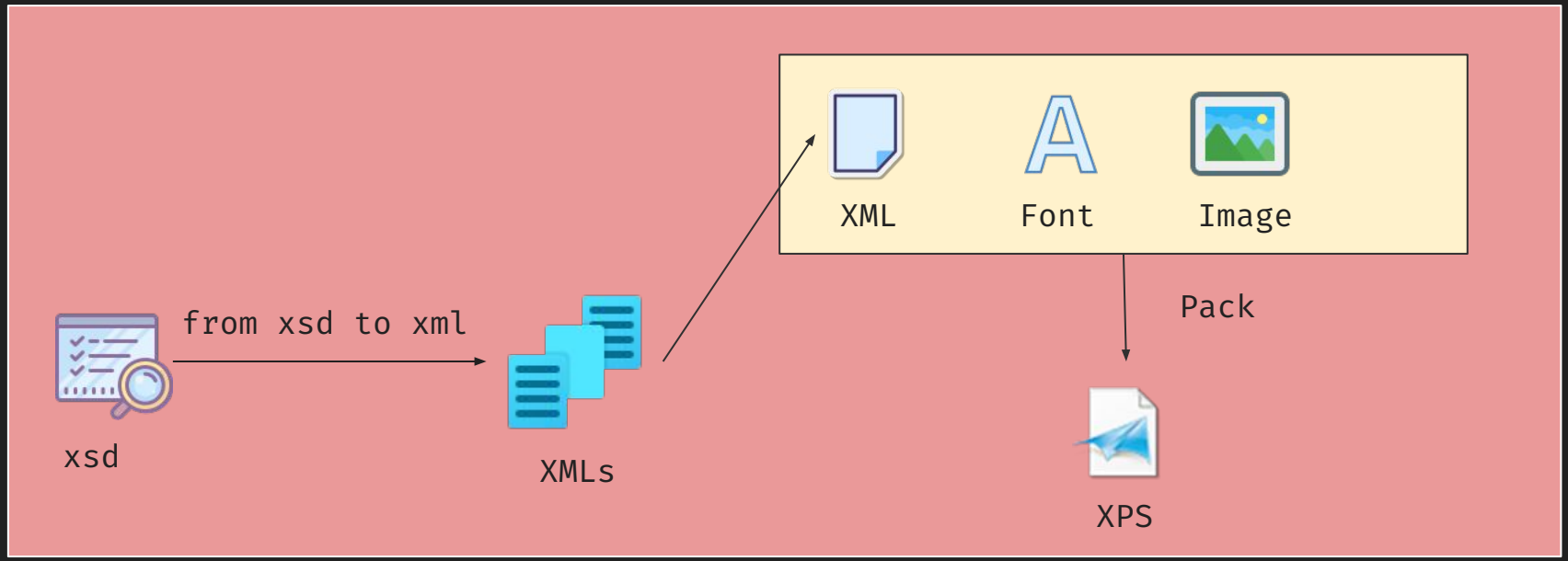
Commonly used to validate XML formats.





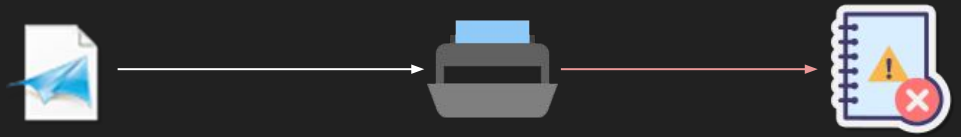
PrintXPS – Input Generation

Use xsd to generate xml



PrintXPS – Document Repair

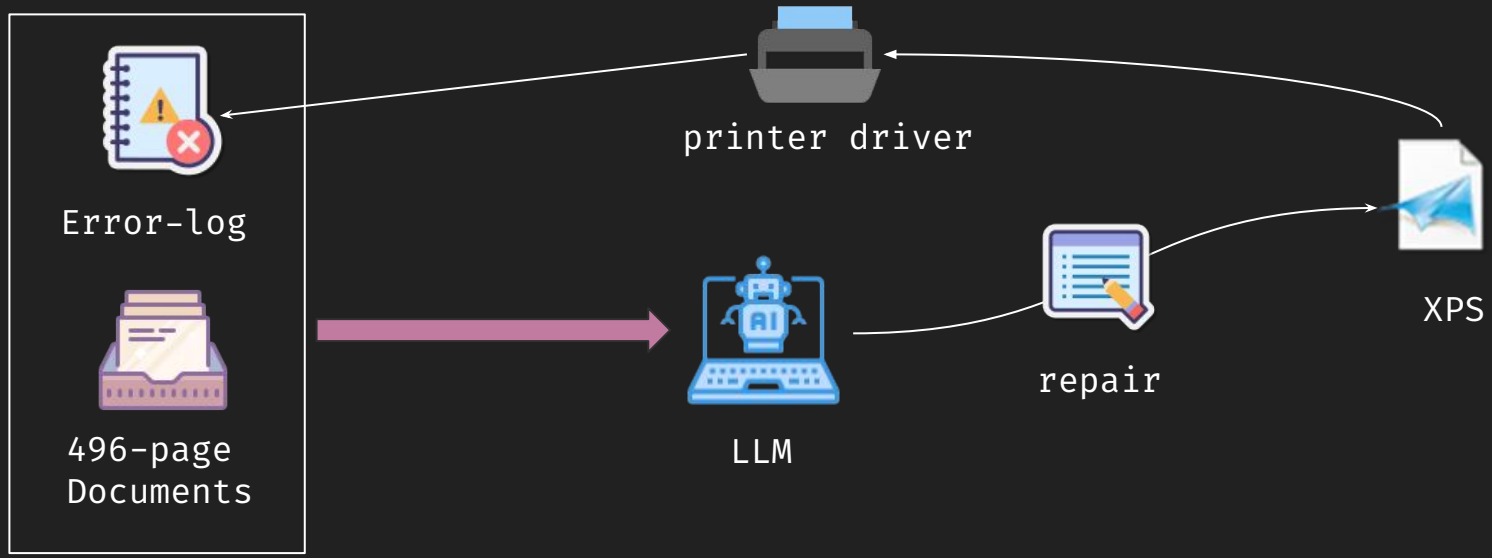
Samples generated by xsd2xml sometimes do not meet the requirements of printer drivers




```
cmnErrorLog::Add(
      2i64,
      1i64,
      2i64,
      "xamlPath::ParseDashes",
      "%ls[%u]: Dash array must have even number
of entries; cnt: %u",
      v15,
      v26,
      v27);
```

PrintXPS – Document Repair

It can be empowered by LLM



CVEs in parsing XML page

Microsoft Printer Driver Remote Code Execution Vulnerability

CVE-2023-24883 CVE-2023-24884 CVE-2023-24885

CVE-2023-24886 CVE-2023-24887 CVE-2023-24924

CVE-2023-24925 CVE-2023-24926 CVE-2023-24927

CVE-2023-24928 CVE-2023-28243

Microsoft Printer Driver Information Disclosure Vulnerability

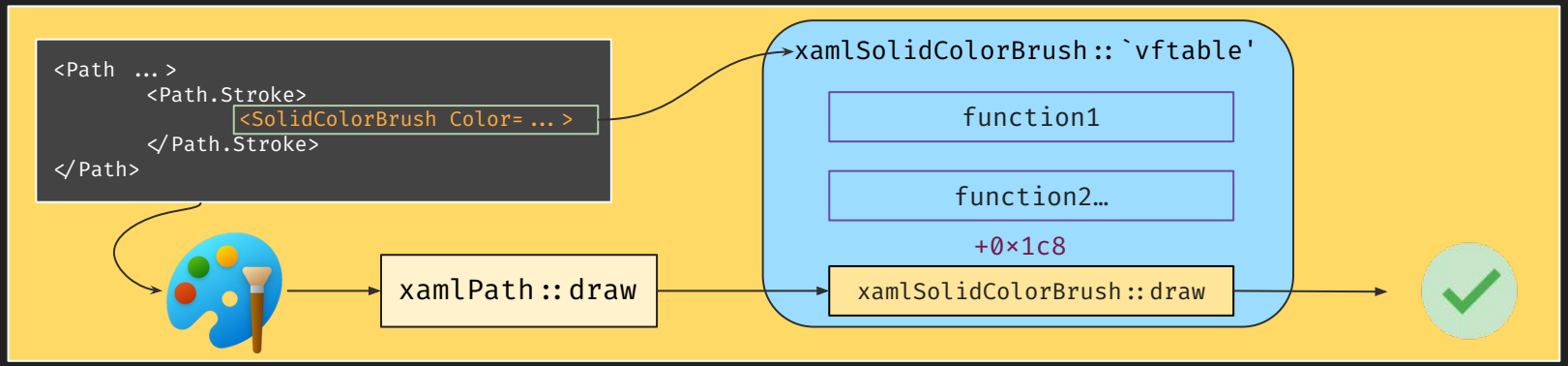
CVE-2023-32085

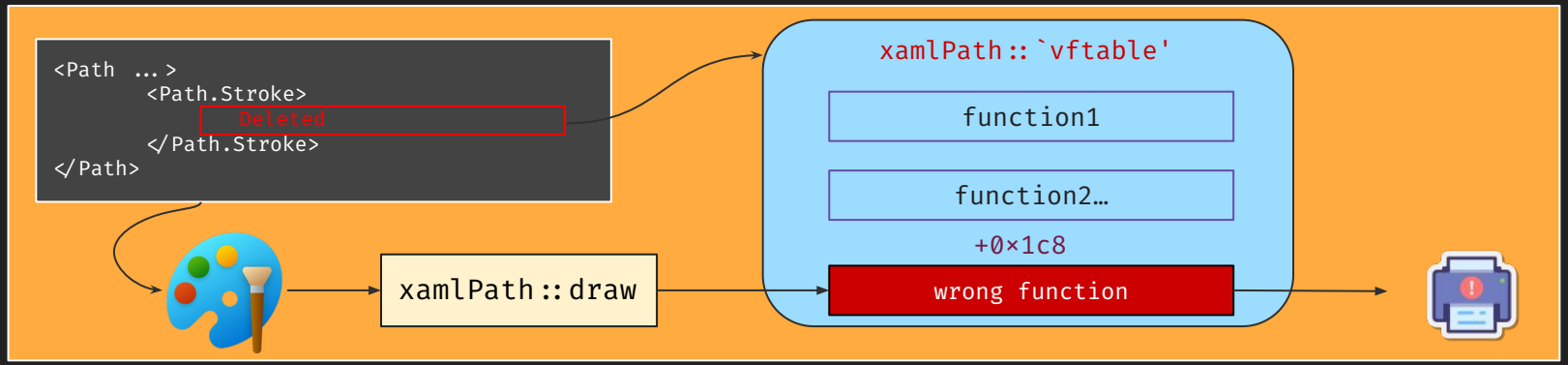
Case 4

CVE-2023-24927 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability

Weakness: CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')

Case 4


<Path ... >
<Path.Stroke>
<SolidColorBrush Color= ... >
</Path.Stroke>
</Path>
xamlSolidColorBrush::`vftable'
function1
function2…
+0×1c8
xamlSolidColorBrush::draw
xamlPath::draw


<Path ... >
<Path.Stroke>
Deleted
</Path.Stroke>
</Path>
xamlPath::`vftable'
function1
function2…
+0×1c8
wrong function
xamlPath::draw

Next

Microsoft fixed their documents

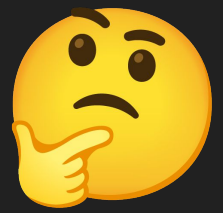
The Manifest file

To use the Windows-provided XPS filters, the v4 driver manifest file must use the RequiredFiles directive under the **DriverConfig** section to specify the filters. These are the names of the filters:

MSxpsPCL6.dll. Provides conversion from XPS to PCL6. *MSxpsPS.dll*. Provides conversion from XPS to PostScript level 3. No INF updates are required to utilize one of these filters, and redistribution is not supported. We recommend users discontinue use of these XPS Filters.

- Vulnerabilities in features Microsoft recommends against using, such as XPS Filters

Is that enough?



Vulnerability in Third-Party Driver

Third-Party Printer Drivers

Some manufacturers still rely on Microsoft's discontinued drivers to assist with their printing

Others have adopted their own custom drivers

Third-Party Printer Drivers

Own custom drivers

...

Rely on Microsoft's

...

CVE in HP Print Driver

Certain HP Print Products–Potential Remote Code Execution and/or Elevation of Privilege with the HP Smart Universal Printing Driver

Client / Server PCs with the HP Smart Universal Printing Driver installed are potentially vulnerable to Remote Code Execution and/or Elevation of Privilege. A client using the HP Smart Universal Printing Driver that sends a print job comprised of a malicious XPS file could potentially lead to Remote Code Execution and/or Elevation of Privilege on the PC.

Scroll to Resolution

Severity
High

HP Reference
HPSBPI03975 Rev. 2

Release date
October 30, 2024

Last updated
October 30, 2024

Category
Print

Potential Security Impact
Potential Remote Code Execution and/or Elevation of Privilege

Relevant Common Vulnerabilities and Exposures (CVE) List
Reported by Zhiniang Peng (@edwardzpeng), devoke@HUST, wh1tc

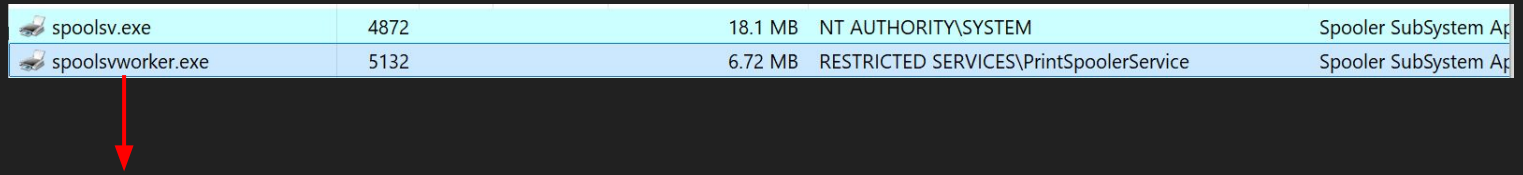
LIST OF CVE IDS

CVE ID	CVSS	Severity	Vector
CVE-2024-9419	7.8	High	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

The new printer

Windows protected print mode (requires manual activation)

- Module blocking
- Per-user XPS rendering
- Lower privileges for common spooler tasks
- Binary mitigations



All print jobs will be handled by the new process, no longer running at SYSTEM

Summary

Summary

Review the old Spooler bugs.

Diving into Spooler again and found a new attack surface.

30+ CVEs in resource parsing, XML parsing and third-party driver.

Will the new print spooler secure in the future?

Takeaway

You can always find new attack surfaces if you dive deep enough.

Spooler is a good attack surface even after years of vulnerabilities disclosure.

Disable your Spooler, if you don’t need it.

Thanks!