Marcin 'Icewall' Noga
http://www.icewall.pl
@_Icewall

PWNing Warszawa 2017

When Third-party components become a source of all evil

Intro

- Yves Younan
  - Research Manager
  - Cisco Talos
- Team
  - Aleksandar Nikolich
  - Ali Rizvi-Santiago
  - Marcin Noga
  - Piotr Bania
  - Tyler Bohan
  - Cory Duplantis
  - Lilith Wyatt
  - Claudio Bozzato

- Talos Vulndev
  - Third party vulnerability research
    - ~ 200 bugów znalezionych w ostatnie 12 miesięcy
    - Microsoft
    - Apple
    - Oracle
    - Adobe
    - Google
    - IBM, HP, Intel, Lexmark
    - 7zip, libarchive, NTP
  - Security tools development
    - Fuzzers, Crash triage
  - Mitigation development

Agenda

- How components „provided/shared” by other providers can affect your product.
- Examples of bugs, misuses, other problems with use of libraries in Enterprise solutions and their consequences.
- Bugs analysis
- Exploitation
- Summary

Talos

Libarchive vs Splunk

Libarchive

- Description
    - Open source library supports read and write operation in a variety of archive formats.
- Motivation
    - Huge number of supported formats (more than 20)
        - zip, rar, 7zip, mtree, cpio, xar, (…)
    - Popularity
        - Package Managers
            - Cmake
            - pkgutils
        - Archiving tools and File Browsers
            - Nautilus
        - Enterprise solutions
            - Splunk

Libarchive – plan of attack

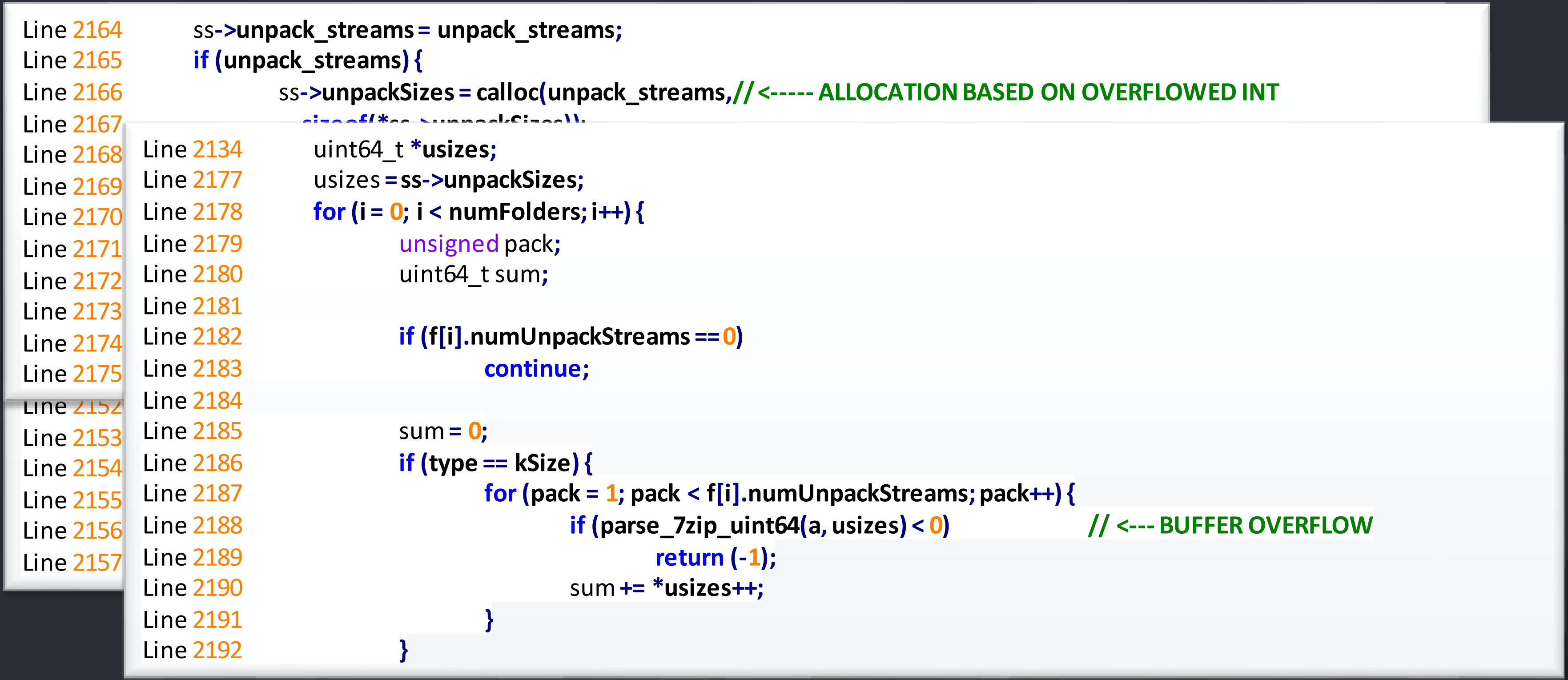
- Used methods to find vulnerabilities
    - A lot of supported formats, opensource, lets do this in a comprehensive way!
        - Fuzzing – using many machines
        - Automatic static code analysis
        - Code review

Libarchive - results

- 4 bugs
- Which method turned out to be the most efficient one ?
  - Fuzzing
    - LIBARCHIVE RAR RESTARTMODEL CODE EXECUTION VULNERABILITY
      - CVE-2016-4302
  - Automatic Static Code Analysis
    - LIBARCHIVE MTREE PARSE_DEVICE CODE EXECUTION VULNERABILITY
      - CVE-2016-4301
  - Code review
    - LIBARCHIVE ZIP ZIP_READ_MAC_METADATA CODE EXECUTION VULNERABILITY
      - CVE-2016-1541
    - LIBARCHIVE 7ZIP READ_SUBSTREAMSINFO CODE EXECUTION VULNERABILITY
      - CVE-2016-4300

Libarchive – bug analysis

- LIBARCHIVE 7ZIP READ_SUBSTREAMSINFO CODE EXECUTION VULNERABILITY
    - Why fuzzer did not find it ?

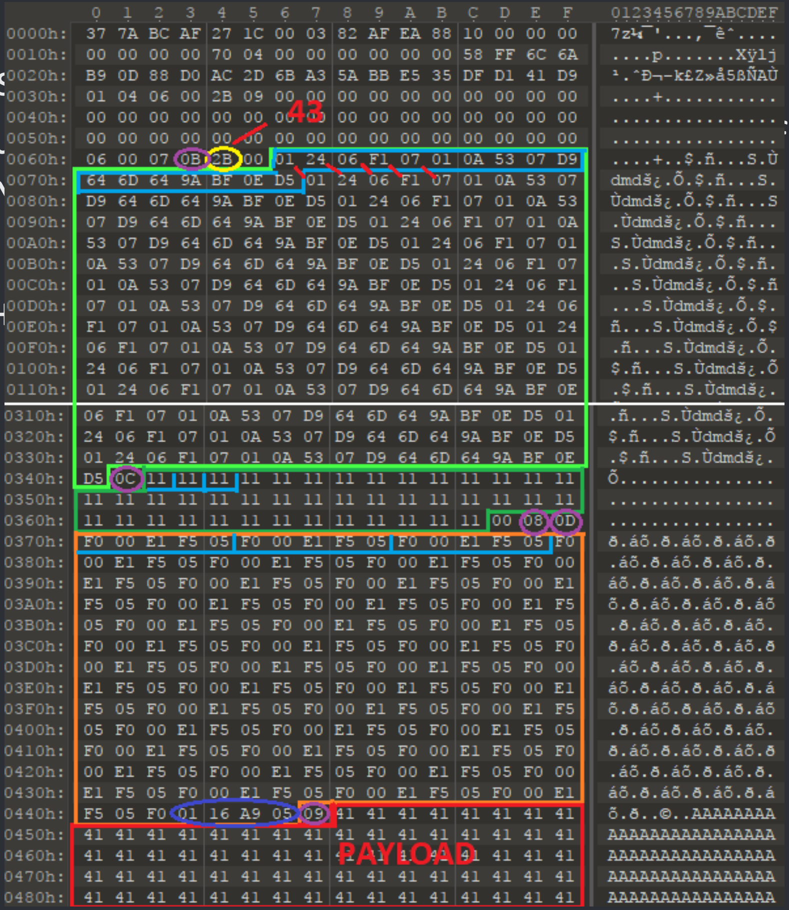


```
ss->unpack_streams = unpack_streams;
if (unpack_streams) {
        ss->unpackSizes = calloc(unpack_streams,// <----- ALLOCATION BASED ON OVERFLOWED INT
            sizeof(*ss->unpackSizes));
```

```
uint64_t *usizes;
usizes = ss->unpackSizes;
for (i = 0; i < numFolders; i++) {
        unsigned pack;
        uint64_t sum;

        if (f[i].numUnpackStreams == 0)
                continue;

        sum = 0;
        if (type == kSize) {
                for (pack = 1; pack < f[i].numUnpackStreams; pack++) {
                        if (parse_7zip_uint64(a, usizes) < 0)            // <--- BUFFER OVERFLOW
                                return (-1);
                        sum += *usizes++;
                }
        }
```

LIBARCHIVE 7ZIP READ_SUBSTREAMSINFO

- 43 at least one s
- Does file with su further modifications ?
- Unfortunatelly N
- So ?
  - Debugger +



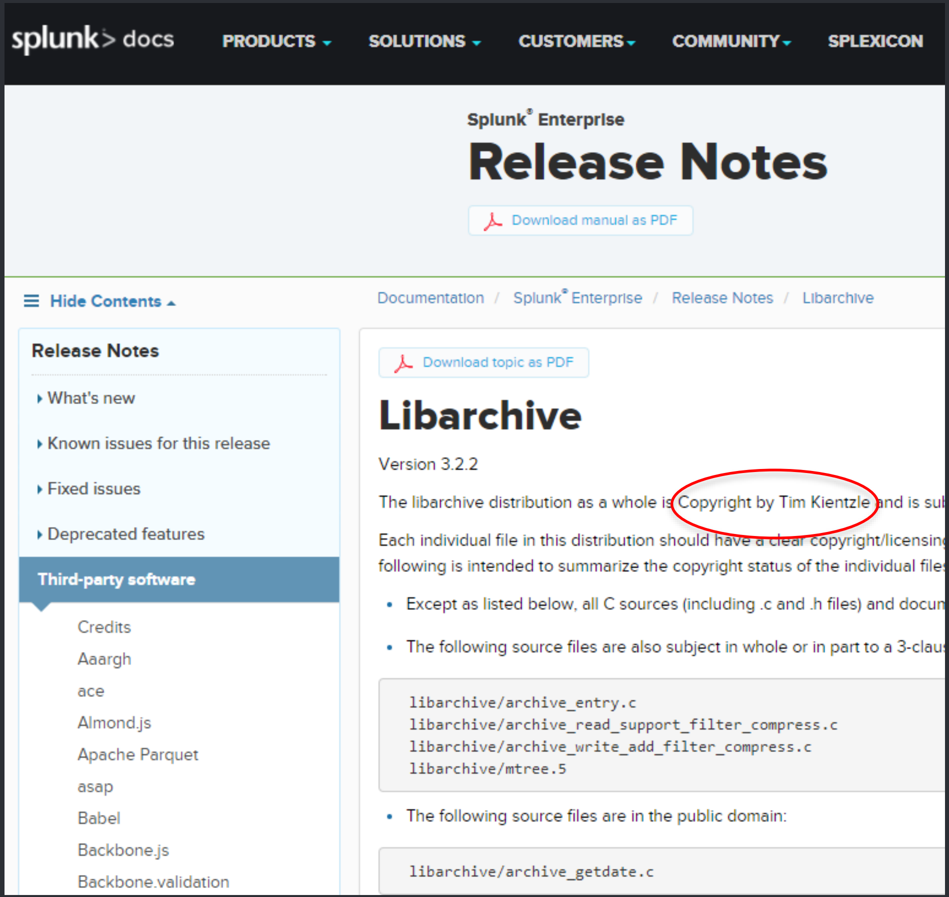
```
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 37 7A BC AF 27 1C 00 03 82 AF EA 88 10 00 00 00  7z¼¯'...‚¯êˆ....
0010h: 00 00 00 00 70 04 00 00 00 00 00 00 58 FF 6C 6A  ....p.......Xÿlj
0020h: B9 0D 88 D0 AC 2D 6B A3 5A BB E5 35 DF D1 41 D9  ¹.ˆÐ¬-k£Z»å5ßÑAÙ
0030h: 01 04 06 00 2B 09 00 00 00 00 00 00 00 00 00 00  ....+...........
0040h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0050h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0060h: 06 00 07 0B 2B 00 01 24 06 F1 07 01 0A 53 07 D9  ....+..$.ñ...S.Ù
0070h: 64 6D 64 9A BF 0E D5 01 24 06 F1 07 01 0A 53 07  dmdš¿.Õ.$.ñ...S.
0080h: D9 64 6D 64 9A BF 0E D5 01 24 06 F1 07 01 0A 53  Ùdmdš¿.Õ.$.ñ...S
0090h: 07 D9 64 6D 64 9A BF 0E D5 01 24 06 F1 07 01 0A  .Ùdmdš¿.Õ.$.ñ...
00A0h: 53 07 D9 64 6D 64 9A BF 0E D5 01 24 06 F1 07 01  S.Ùdmdš¿.Õ.$.ñ..
00B0h: 0A 53 07 D9 64 6D 64 9A BF 0E D5 01 24 06 F1 07  .S.Ùdmdš¿.Õ.$.ñ.
00C0h: 01 0A 53 07 D9 64 6D 64 9A BF 0E D5 01 24 06 F1  ..S.Ùdmdš¿.Õ.$.ñ
00D0h: 07 01 0A 53 07 D9 64 6D 64 9A BF 0E D5 01 24 06  ...S.Ùdmdš¿.Õ.$.
00E0h: F1 07 01 0A 53 07 D9 64 6D 64 9A BF 0E D5 01 24  ñ...S.Ùdmdš¿.Õ.$
00F0h: 06 F1 07 01 0A 53 07 D9 64 6D 64 9A BF 0E D5 01  .ñ...S.Ùdmdš¿.Õ.
0100h: 24 06 F1 07 01 0A 53 07 D9 64 6D 64 9A BF 0E D5  $.ñ...S.Ùdmdš¿.Õ
0110h: 01 24 06 F1 07 01 0A 53 07 D9 64 6D 64 9A BF 0E  .$.ñ...S.Ùdmdš¿.
0310h: 06 F1 07 01 0A 53 07 D9 64 6D 64 9A BF 0E D5 01  .ñ...S.Ùdmdš¿.Õ.
0320h: 24 06 F1 07 01 0A 53 07 D9 64 6D 64 9A BF 0E D5  $.ñ...S.Ùdmdš¿.Õ
0330h: 01 24 06 F1 07 01 0A 53 07 D9 64 6D 64 9A BF 0E  .$.ñ...S.Ùdmdš¿.
0340h: D5 0C 11 11 11 11 11 11 11 11 11 11 11 11 11 11  Õ...............
0350h: 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11  ................
0360h: 11 11 11 11 11 11 11 11 11 11 11 11 11 00 08 0D  ................
0370h: F0 00 E1 F5 05 F0 00 E1 F5 05 F0 00 E1 F5 05 F0  ð.áõ.ð.áõ.ð.áõ.ð
0380h: 00 E1 F5 05 F0 00 E1 F5 05 F0 00 E1 F5 05 F0 00  .áõ.ð.áõ.ð.áõ.ð.
0390h: E1 F5 05 F0 00 E1 F5 05 F0 00 E1 F5 05 F0 00 E1  áõ.ð.áõ.ð.áõ.ð.á
03A0h: F5 05 F0 00 E1 F5 05 F0 00 E1 F5 05 F0 00 E1 F5  õ.ð.áõ.ð.áõ.ð.áõ
03B0h: 05 F0 00 E1 F5 05 F0 00 E1 F5 05 F0 00 E1 F5 05  .ð.áõ.ð.áõ.ð.áõ.
03C0h: F0 00 E1 F5 05 F0 00 E1 F5 05 F0 00 E1 F5 05 F0  ð.áõ.ð.áõ.ð.áõ.ð
03D0h: 00 E1 F5 05 F0 00 E1 F5 05 F0 00 E1 F5 05 F0 00  .áõ.ð.áõ.ð.áõ.ð.
03E0h: E1 F5 05 F0 00 E1 F5 05 F0 00 E1 F5 05 F0 00 E1  áõ.ð.áõ.ð.áõ.ð.á
03F0h: F5 05 F0 00 E1 F5 05 F0 00 E1 F5 05 F0 00 E1 F5  õ.ð.áõ.ð.áõ.ð.áõ
0400h: 05 F0 00 E1 F5 05 F0 00 E1 F5 05 F0 00 E1 F5 05  .ð.áõ.ð.áõ.ð.áõ.
0410h: F0 00 E1 F5 05 F0 00 E1 F5 05 F0 00 E1 F5 05 F0  ð.áõ.ð.áõ.ð.áõ.ð
0420h: 00 E1 F5 05 F0 00 E1 F5 05 F0 00 E1 F5 05 F0 00  .áõ.ð.áõ.ð.áõ.ð.
0430h: E1 F5 05 F0 00 E1 F5 05 F0 00 E1 F5 05 F0 00 E1  áõ.ð.áõ.ð.áõ.ð.á
0440h: F5 05 F0 01 16 A9 05 09 41 41 41 41 41 41 41 41  õ.ð..©..AAAAAAAA
0450h: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0460h: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0470h: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0480h: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
```

Libarchive vs Splunk

- Splunk?
  - „Allows logs aggregations from many sources, formats and their analysis”

- How I discovered that Splunk uses libarchive ?
  - General HINT’s
  - Google for one of specific strings from COPYING, COPYRIGTHS, LICENSE files
    - e.g. : „Copyright by Tim Kientzle”
    - or general „Third-party software ComponentName”

Libarchive vs Splunk



Splunk® Enterprise

Release Notes

Release Notes

- What's new
- Known issues for this release
- Fixed issues
- Deprecated features

Third-party software

- Credits
- Aaargh
- ace
- Almond.js
- Apache Parquet
- asap
- Babel
- Backbone.js
- Backbone.validation

Libarchive

Version 3.2.2

The libarchive distribution as a whole is Copyright by Tim Kientzle and is sul

Each individual file in this distribution should have a clear copyright/licensing following is intended to summarize the copyright status of the individual files

- Except as listed below, all C sources (including .c and .h files) and docum
- The following source files are also subject in whole or in part to a 3-claus

```
libarchive/archive_entry.c
libarchive/archive_read_support_filter_compress.c
libarchive/archive_write_add_filter_compress.c
libarchive/mtree.5
```

- The following source files are in the public domain:

```
libarchive/archive_getdate.c
```

Libarchive vs Splunk

- How to trigger the vulnerability ?
    - Two potential vectors
        - archive in directory with logs
            - by default only zip
        - upload kmz file (zip) in Splunk’s web panel.

- Where exactly libarchive is used ?
    - hackers-grep
        - hackers-grep.py -n c:\splunk .*.exe "archive_read_open”
            - splunkd.exe

Splunk suicide

- Libarchive allows to active support for particular formats or for all available.
- Splunk's authors have choosen the second options == bypass of file extensin limitation defined in confiugration file.

```
struct archive *a;
a = archive_read_new();

if( strcmp("7zip",formatName) == 0 ) { archive_read_support_format_7zip(a); }
if( strcmp("cab",formatName) == 0 ) { archive_read_support_format_cab(a); }
if( strcmp("rar",formatName) == 0 ) { archive_read_support_format_rar(a); }
if( strcmp("iso9660",formatName) == 0 ) { archive_read_support_format_iso9660(a); }
if( strcmp("zip",formatName) == 0 ) { archive_read_support_format_zip(a); }
(...)

 vs

archive_read_support_format_all(a);
```

Splunk video

- Autorzy splunk’a zdecydowali się aktywować wszystkie dostępne formaty
  - Zwiększenie ilości wektorów ataku

PLAY

MarkLogic
vs
„Converters”

Looking for a target ...

- Google „metadata extraction”
- I found MarkLogic documentation page

> MarkLogic Server server offers the XQuery built-in, xdmp:document-filter, to extract and associate metadata from binary documents: These functions extract metadata and text from binary documents as XHTML.

- Supported file formats:
    - Presentation
    - Raster Image
    - Spreadsheet
    - Archives
    - Word Processing and General Office
    - (...)

MarkLogic

- Description
  - NoSQL database – non-relational database, focused on aggregation large amount of different type data (BigData)
- What BigData is ?
  - „massive” amount of different kind of data, which processing (PARSING) can provide valuable informations.
- Customers list
  - http://www.marklogic.com/customers/

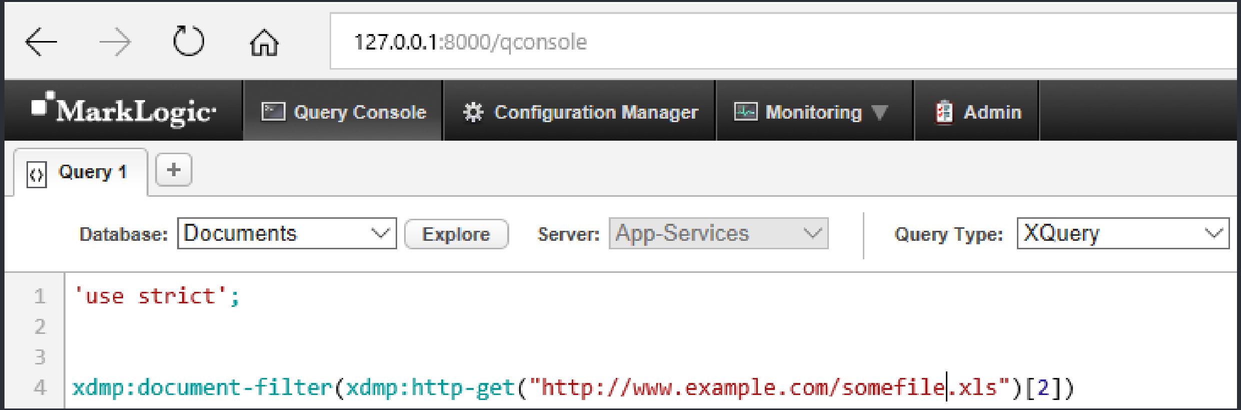
gov

finanse

tv

Where exactly metadata are extracted ?

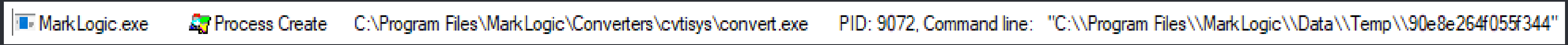
- Example of xdmp:document-filter call



Database: Documents Server: App-Services Query Type: XQuery

```
'use strict';


xdmp:document-filter(xdmp:http-get("http://www.example.com/somefile.xls")[2])
```

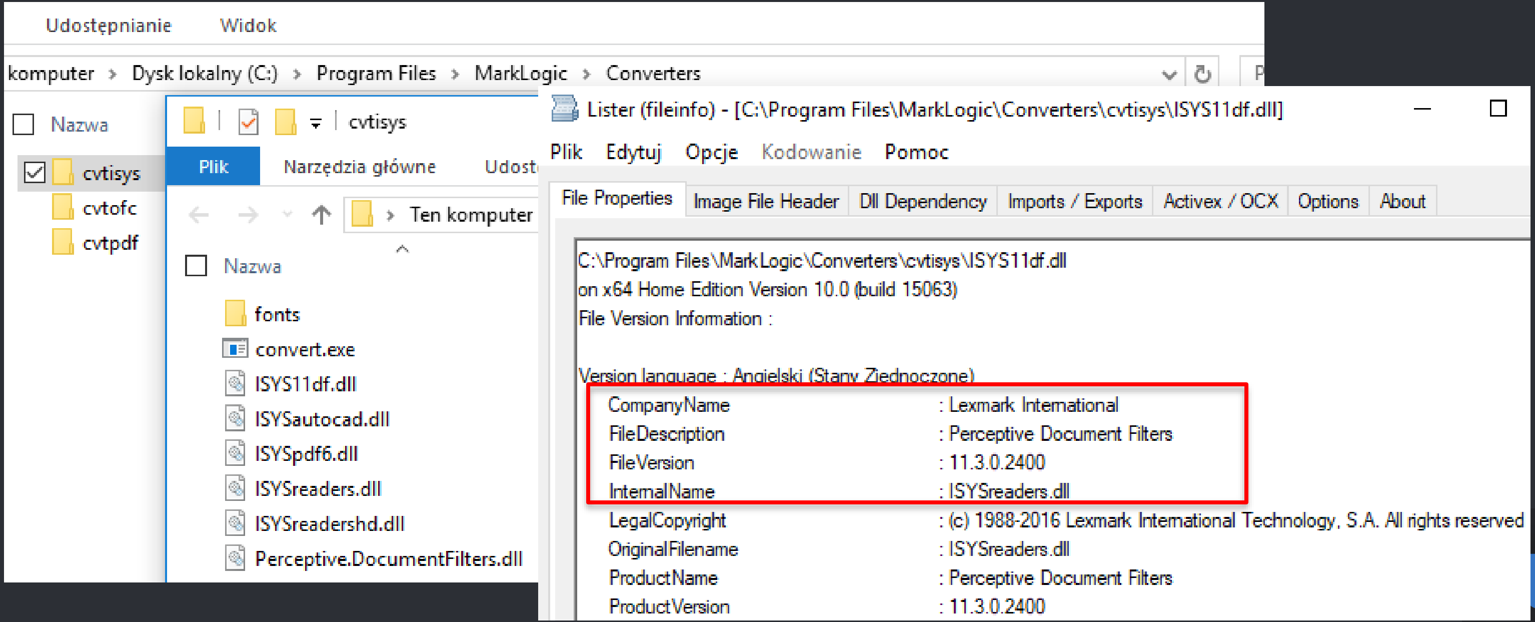
- Process Monitor



```
MarkLogic.exe    Process Create    C:\Program Files\MarkLogic\Converters\cvtisys\convert.exe    PID: 9072, Command line:   "C:\\Program Files\\MarkLogic\\Data\\Temp\\90e8e264f055f344"
```

So converters …

- 3 converters
- To get more info about files we can :
  - Google for file names
  - Check info in resource directories



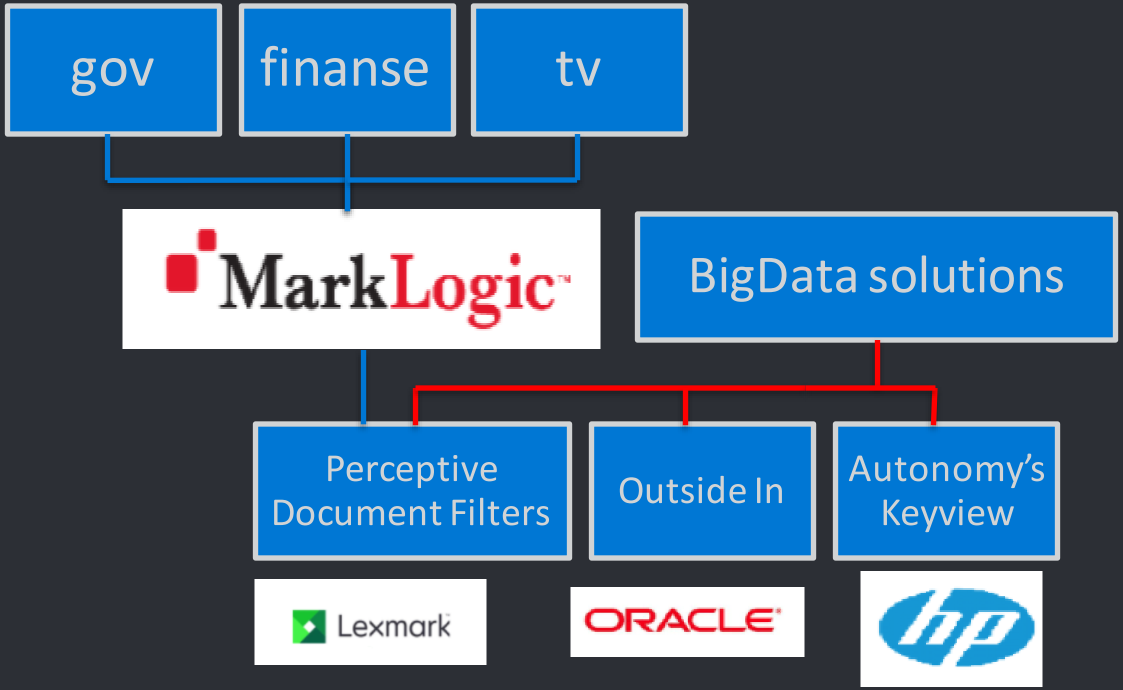
```
C:\Program Files\MarkLogic\Converters\cvtisys\ISYS11df.dll
on x64 Home Edition Version 10.0 (build 15063)
File Version Information :

Version language : Angielski (Stany Zjednoczone)
    CompanyName                    : Lexmark International
    FileDescription                : Perceptive Document Filters
    FileVersion                    : 11.3.0.2400
    InternalName                   : ISYSreaders.dll
    LegalCopyright                 : (c) 1988-2016 Lexmark International Technology, S.A. All rights reserved
    OriginalFilename               : ISYSreaders.dll
    ProductName                    : Perceptive Document Filters
    ProductVersion                 : 11.3.0.2400
```

Perceptive Document Filters

- Description
  - Owner
    - Lexmark
  - Set of libraries providing abilities for :
    - File type identification
    - Metadata extraction
    - Archive decompression
    - (...)
  - ~ 100 supported formats
  - Commercial
  - Close source

BigData

- Three major players providing SDK (libraries,...) for BigData solutions.



gov

finanse

tv

MarkLogic

BigData solutions

Perceptive Document Filters

Outside In

Autonomy's Keyview

Lexmark

ORACLE

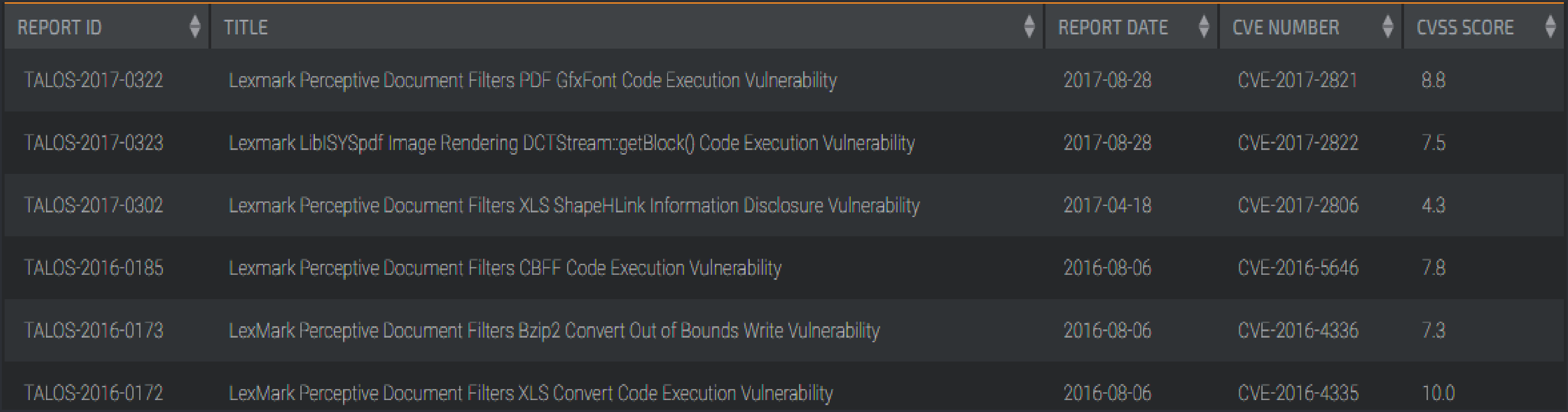
hp

Discovered bugs

- Lexmark – Perceptive Document Filters
  - 6 CVE
- Oracle – Outside In (OIT)
  - 17 CVE
- HP – Autonomy’s KeyView
  - 4 CVE

Perceptive Document Filters - results

- 6 bugs

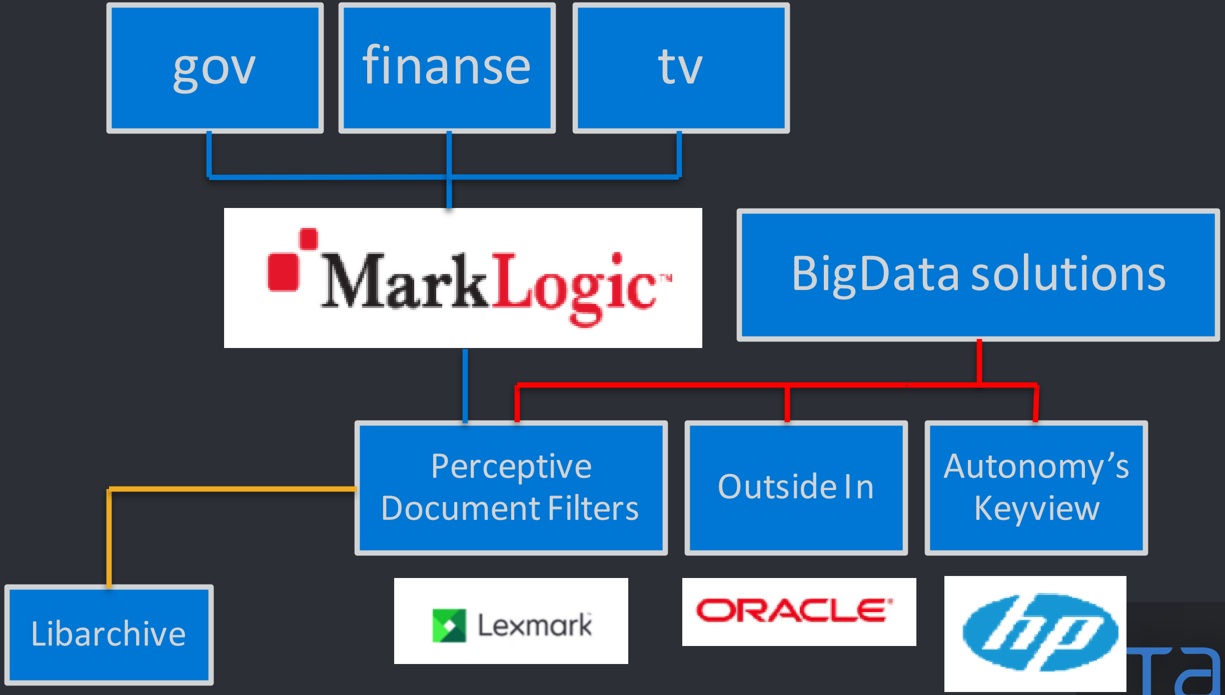


REPORT ID	TITLE	REPORT DATE	CVE NUMBER	CVSS SCORE
TALOS-2017-0322	Lexmark Perceptive Document Filters PDF GfxFont Code Execution Vulnerability	2017-08-28	CVE-2017-2821	8.8
TALOS-2017-0323	Lexmark LibISYSpdf Image Rendering DCTStream::getBlock() Code Execution Vulnerability	2017-08-28	CVE-2017-2822	7.5
TALOS-2017-0302	Lexmark Perceptive Document Filters XLS ShapeHLink Information Disclosure Vulnerability	2017-04-18	CVE-2017-2806	4.3
TALOS-2016-0185	Lexmark Perceptive Document Filters CBFF Code Execution Vulnerability	2016-08-06	CVE-2016-5646	7.8
TALOS-2016-0173	LexMark Perceptive Document Filters Bzip2 Convert Out of Bounds Write Vulnerability	2016-08-06	CVE-2016-4336	7.3
TALOS-2016-0172	LexMark Perceptive Document Filters XLS Convert Code Execution Vulnerability	2016-08-06	CVE-2016-4335	10.0

- Used methods to find vulnerabilities
  - Fuzzing / cross fuzzing
  - Mainly used files : doc, xls, ppt
    - initialy also archive files (using corpus from libarchive), but ...

Components inception

- First crash in Perceptive Doc. Filters revealed that it uses libarchie for archive decompression.



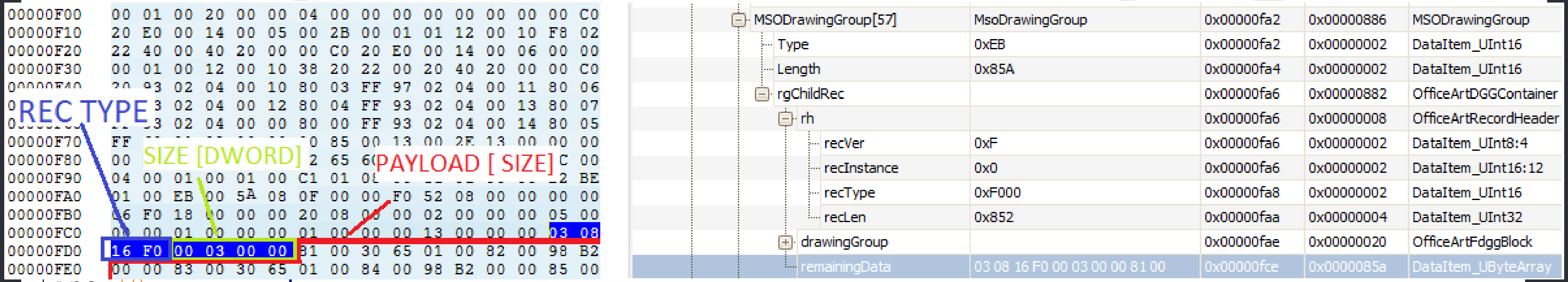
TALOS

Perceptive Document Filters – bug analysis

- LexMark Perceptive Document Filters XLS Convert Code Execution Vulnerability
  - CVE-2016-4335
- Vulnerable function
  - reader::escher::MsofbtDggContainer::Handle
- Library
  - libISYSreadershd.so
- Type of vulnerability
  - Stack Based Buffer Overflow

Perceptive Document Filters – bug analysis

```
struct_a1 * reader::escher::MsofbtDggContainer::Handle(struct_a1 *a1, __int64 *a2,
```



```
00000F00   00 01 00 20 00 00 04 00 00 00 00 00 00 00 00 C0
00000F10   20 E0 00 14 00 05 00 2B 00 01 01 12 00 10 F8 02
00000F20   22 40 00 40 20 00 00 C0 20 E0 00 14 00 06 00 00
00000F30   00 01 00 12 00 10 38 20 22 00 20 40 20 00 00 C0
00000F40   20 93 02 04 00 10 80 03 FF 97 02 04 00 11 80 06
              3 02 04 00 12 80 04 FF 93 02 04 00 13 80 07
              3 02 04 00 00 80 00 FF 93 02 04 00 14 80 05
00000F70   FF                   0 85 00 13 00 2E 13 00 00 00
00000F80   00                   2 65 6                 C 00
00000F90   04 00 01 00 01 00 C1 01 08                   2 BE
00000FA0   01 00 EB 00 5A 08 0F 00 00 F0 52 08 00 00 00 00
00000FB0   06 F0 18 00 00 00 20 08 00 00 02 00 00 00 05 00
00000FC0   00 00 01 00 00 00 01 00 00 00 13 00 00 00 03 08
00000FD0   16 F0 00 03 00 00 81 00 30 65 01 00 82 00 98 B2
00000FE0   00 00 83 00 30 65 01 00 84 00 98 B2 00 00 85 00
```

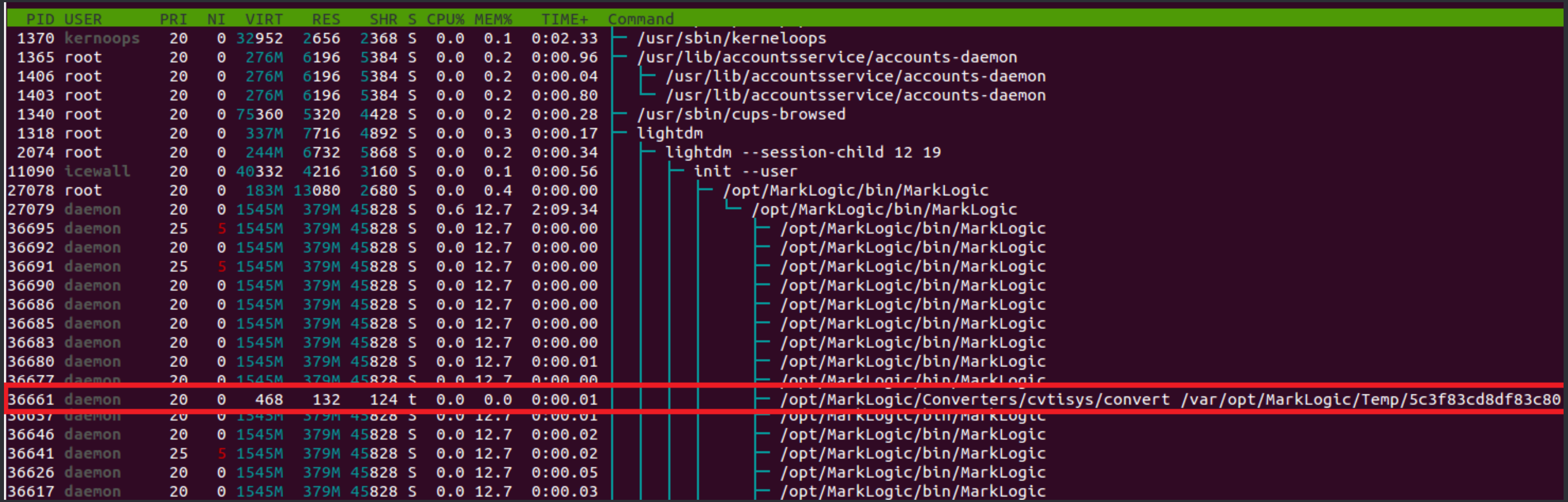
MSODrawingGroup[57]	MsoDrawingGroup	0x00000fa2	0x00000886	MSODrawingGroup
Type	0xEB	0x00000fa2	0x00000002	DataItem_UInt16
Length	0x85A	0x00000fa4	0x00000002	DataItem_UInt16
rgChildRec		0x00000fa6	0x00000882	OfficeArtDGGContainer
rh		0x00000fa6	0x00000008	OfficeArtRecordHeader
recVer	0xF	0x00000fa6	0x00000002	DataItem_UInt8:4
recInstance	0x0	0x00000fa6	0x00000002	DataItem_UInt16:12
recType	0xF000	0x00000fa8	0x00000002	DataItem_UInt16
recLen	0x852	0x00000faa	0x00000004	DataItem_UInt32
drawingGroup		0x00000fae	0x00000020	OfficeArtFdggBlock
remainingData	03 08 16 F0 00 03 00 00 81 00	0x00000fce	0x0000085a	DataItem_UByteArray

```
                }
                if ( recType == 0xF016u )
                {
                  CPageMemoryStream::Read(&localBuffer, MSOFBH_header->size)
```

Exploitation

CVE-2016-4335

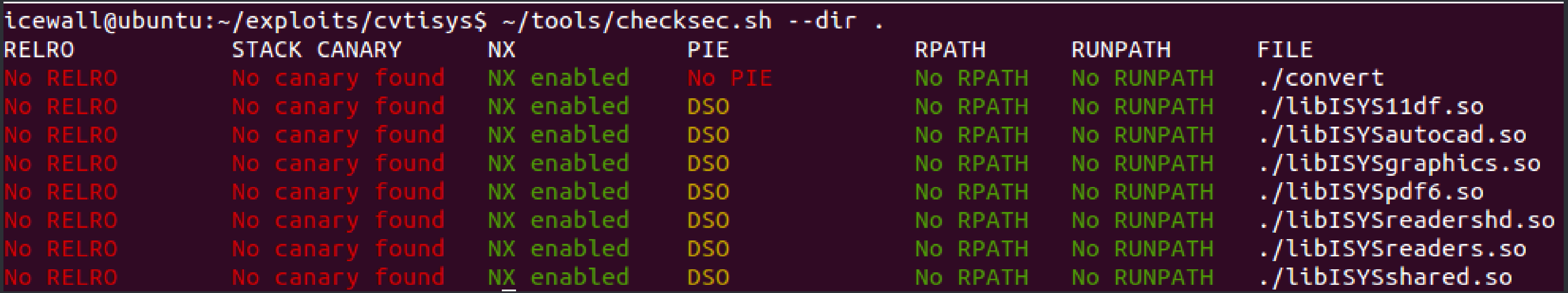
Just after xdmp:document-filter API call



```
  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
 1370 kernoops   20   0 32952  2656  2368 S  0.0  0.1  0:02.33 ├─ /usr/sbin/kerneloops
 1365 root       20   0  276M  6196  5384 S  0.0  0.2  0:00.96 ├─ /usr/lib/accountsservice/accounts-daemon
 1406 root       20   0  276M  6196  5384 S  0.0  0.2  0:00.04 │  ├─ /usr/lib/accountsservice/accounts-daemon
 1403 root       20   0  276M  6196  5384 S  0.0  0.2  0:00.80 │  └─ /usr/lib/accountsservice/accounts-daemon
 1340 root       20   0 75360  5320  4428 S  0.0  0.2  0:00.28 ├─ /usr/sbin/cups-browsed
 1318 root       20   0  337M  7716  4892 S  0.0  0.3  0:00.17 ├─ lightdm
 2074 root       20   0  244M  6732  5868 S  0.0  0.2  0:00.34 │  ├─ lightdm --session-child 12 19
11090 icewall    20   0 40332  4216  3160 S  0.0  0.1  0:00.56 │  │  ├─ init --user
27078 root       20   0  183M 13080  2680 S  0.0  0.4  0:00.00 │  │  │  ├─ /opt/MarkLogic/bin/MarkLogic
27079 daemon     20   0 1545M  379M 45828 S  0.6 12.7  2:09.34 │  │  │  │  └─ /opt/MarkLogic/bin/MarkLogic
36695 daemon     25   5 1545M  379M 45828 S  0.0 12.7  0:00.00 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
36692 daemon     20   0 1545M  379M 45828 S  0.0 12.7  0:00.00 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
36691 daemon     25   5 1545M  379M 45828 S  0.0 12.7  0:00.00 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
36690 daemon     20   0 1545M  379M 45828 S  0.0 12.7  0:00.00 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
36686 daemon     20   0 1545M  379M 45828 S  0.0 12.7  0:00.00 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
36685 daemon     20   0 1545M  379M 45828 S  0.0 12.7  0:00.00 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
36683 daemon     20   0 1545M  379M 45828 S  0.0 12.7  0:00.00 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
36680 daemon     20   0 1545M  379M 45828 S  0.0 12.7  0:00.01 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
36677 daemon     20   0 1545M  379M 45828 S  0.0 12.7  0:00.00 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
36661 daemon     20   0   468   132   124 t  0.0  0.0  0:00.01 │  │  │  │     ├─ /opt/MarkLogic/Converters/cvtisys/convert /var/opt/MarkLogic/Temp/5c3f83cd8df83c80
36657 daemon     20   0 1545M  379M 45828 S  0.0 12.7  0:00.01 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
36646 daemon     20   0 1545M  379M 45828 S  0.0 12.7  0:00.02 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
36641 daemon     25   5 1545M  379M 45828 S  0.0 12.7  0:00.02 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
36626 daemon     20   0 1545M  379M 45828 S  0.0 12.7  0:00.05 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
36617 daemon     20   0 1545M  379M 45828 S  0.0 12.7  0:00.03 │  │  │  │     ├─ /opt/MarkLogic/bin/MarkLogic
```

Process **convert** executed with **daemon** privilages.

Perceptive Doc. Filters – mitigations check



```
icewall@ubuntu:~/exploits/cvtisys$ ~/tools/checksec.sh --dir .
RELRO           STACK CANARY      NX            PIE             RPATH      RUNPATH      FILE
No RELRO        No canary found   NX enabled    No PIE          No RPATH   No RUNPATH   ./convert
No RELRO        No canary found   NX enabled    DSO             No RPATH   No RUNPATH   ./libISYS11df.so
No RELRO        No canary found   NX enabled    DSO             No RPATH   No RUNPATH   ./libISYSautocad.so
No RELRO        No canary found   NX enabled    DSO             No RPATH   No RUNPATH   ./libISYSgraphics.so
No RELRO        No canary found   NX enabled    DSO             No RPATH   No RUNPATH   ./libISYSpdf6.so
No RELRO        No canary found   NX enabled    DSO             No RPATH   No RUNPATH   ./libISYSreadershd.so
No RELRO        No canary found   NX enabled    DSO             No RPATH   No RUNPATH   ./libISYSreaders.so
No RELRO        No canary found   NX enabled    DSO             No RPATH   No RUNPATH   ./libISYSshared.so
```

Exploitation strategy

- Trigger the vulnerability via xdmp:document-filter API.
- Convert binary does not drop privilages == auto priv escal
- Convert
  - created by MarkLogic
  - lack of ASLR
- ROP (DEP bypass)
- Remote Shell!

- Full exploitation write-up:
- http://blog.talosintelligence.com/2017/06/lexmark-perceptive-vuln-deep-dive.html

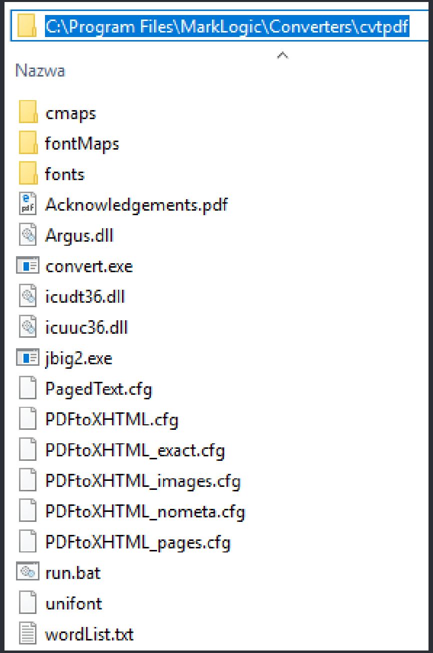
„ Deep dive in Lexmark Perceptive Document Filters Exploitation”

MarkLogic 0wn3d via Perceptive Doc. Filters

VIDEO

Iceni Argus PDF

- Description
  - Owner
    - Iceni
  - Commercial
  - Close source
  - Its purpose as MarkLogic component:
    - Extraction of PDF content
    - Conversion PDF to XHTML
  - Related API:
    - xdmp:pdf-convert



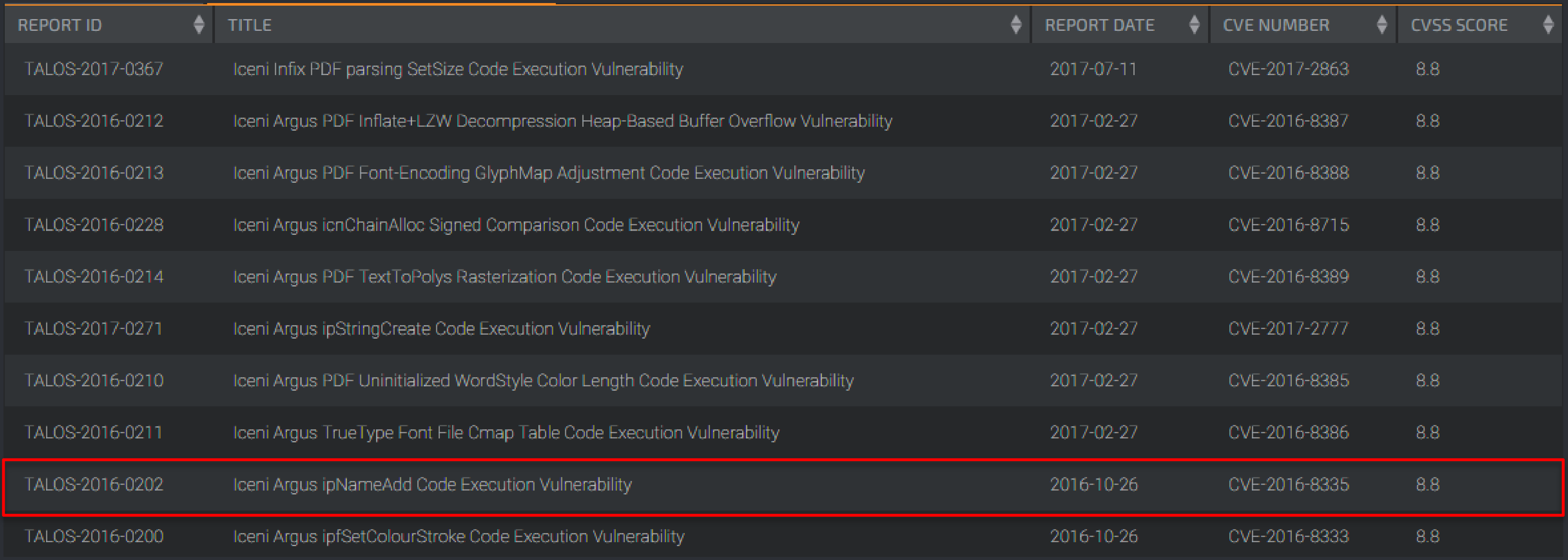
C:\Program Files\MarkLogic\Converters\cvtpdf

Nazwa

cmaps
fontMaps
fonts
Acknowledgements.pdf
Argus.dll
convert.exe
icudt36.dll
icuuc36.dll
jbig2.exe
PagedText.cfg
PDFtoXHTML.cfg
PDFtoXHTML_exact.cfg
PDFtoXHTML_images.cfg
PDFtoXHTML_nometa.cfg
PDFtoXHTML_pages.cfg
run.bat
unifont
wordList.txt

Iceni Argus PDF – fuzzing results

- 10 bugs

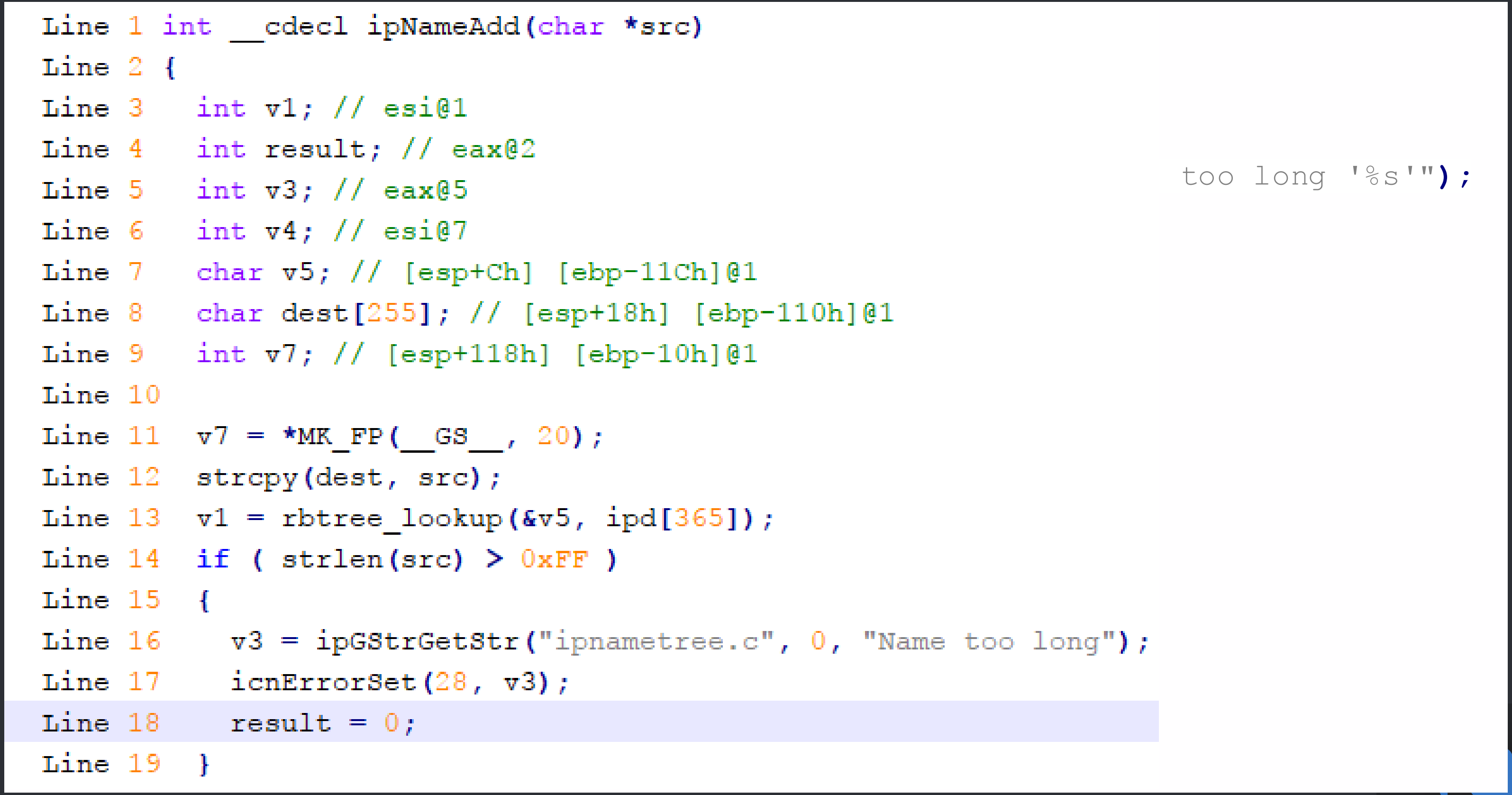


REPORT ID	TITLE	REPORT DATE	CVE NUMBER	CVSS SCORE
TALOS-2017-0367	Iceni Infix PDF parsing SetSize Code Execution Vulnerability	2017-07-11	CVE-2017-2863	8.8
TALOS-2016-0212	Iceni Argus PDF Inflate+LZW Decompression Heap-Based Buffer Overflow Vulnerability	2017-02-27	CVE-2016-8387	8.8
TALOS-2016-0213	Iceni Argus PDF Font-Encoding GlyphMap Adjustment Code Execution Vulnerability	2017-02-27	CVE-2016-8388	8.8
TALOS-2016-0228	Iceni Argus icnChainAlloc Signed Comparison Code Execution Vulnerability	2017-02-27	CVE-2016-8715	8.8
TALOS-2016-0214	Iceni Argus PDF TextToPolys Rasterization Code Execution Vulnerability	2017-02-27	CVE-2016-8389	8.8
TALOS-2017-0271	Iceni Argus ipStringCreate Code Execution Vulnerability	2017-02-27	CVE-2017-2777	8.8
TALOS-2016-0210	Iceni Argus PDF Uninitialized WordStyle Color Length Code Execution Vulnerability	2017-02-27	CVE-2016-8385	8.8
TALOS-2016-0211	Iceni Argus TrueType Font File Cmap Table Code Execution Vulnerability	2017-02-27	CVE-2016-8386	8.8
TALOS-2016-0202	Iceni Argus ipNameAdd Code Execution Vulnerability	2016-10-26	CVE-2016-8335	8.8
TALOS-2016-0200	Iceni Argus ipfSetColourStroke Code Execution Vulnerability	2016-10-26	CVE-2016-8333	8.8

Iceni Argus PDF – bug analysis

- Iceni Argus ipNameAdd Code Execution Vulnerability
  - CVE-2016-8335
- Vulnerable function
  - ipNameAdd
- Type of vulnerability
  - Stack Based Buffer Overflow
- Library
  - Argus.dll/so

Iceni Argus PDF – bug analysis



```
int __cdecl ipNameAdd(char *src)
{
  int v1; // esi@1
  int result; // eax@2
  int v3; // eax@5
  int v4; // esi@7
  char v5; // [esp+Ch] [ebp-11Ch]@1
  char dest[255]; // [esp+18h] [ebp-110h]@1
  int v7; // [esp+118h] [ebp-10h]@1

  v7 = *MK_FP(__GS__, 20);
  strcpy(dest, src);
  v1 = rbtree_lookup(&v5, ipd[365]);
  if ( strlen(src) > 0xFF )
  {
    v3 = ipGStrGetStr("ipnametree.c", 0, "Name too long");
    icnErrorSet(28, v3);
    result = 0;
  }
```

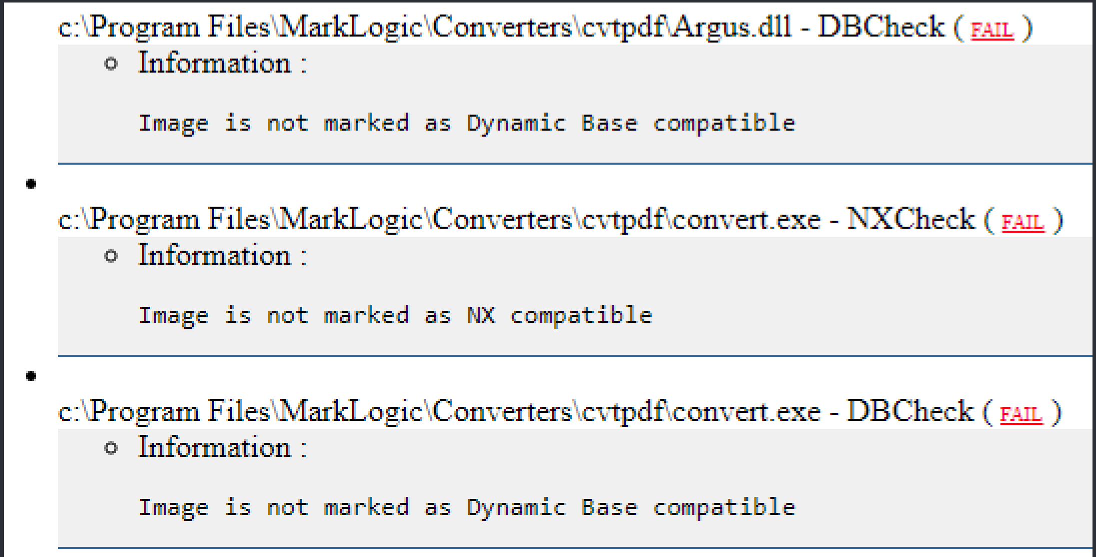
```
too long '%s'");
```

Exploitation

CVE-2016-8335

Maybe this time Windows ?

- Check of implemented Mitigations
  - Results from BinScope'a



c:\Program Files\MarkLogic\Converters\cvtpdf\Argus.dll - DBCheck (FAIL)

- Information :

```
Image is not marked as Dynamic Base compatible
```

c:\Program Files\MarkLogic\Converters\cvtpdf\convert.exe - NXCheck (FAIL)

- Information :

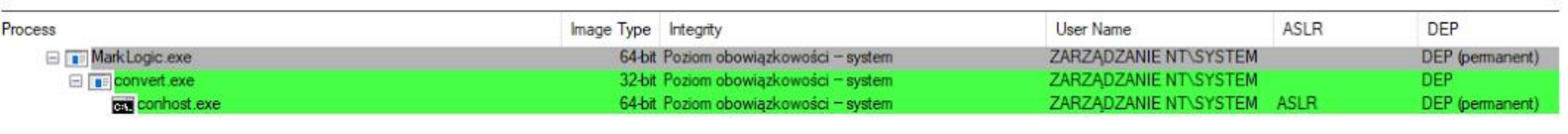
```
Image is not marked as NX compatible
```

c:\Program Files\MarkLogic\Converters\cvtpdf\convert.exe - DBCheck (FAIL)

- Information :

```
Image is not marked as Dynamic Base compatible
```

Remote SYSTEM ?



Process	Image Type	Integrity	User Name	ASLR	DEP
MarkLogic.exe	64-bit	Poziom obowiązkowości – system	ZARZĄDZANIE NT\SYSTEM		DEP (permanent)
convert.exe	32-bit	Poziom obowiązkowości – system	ZARZĄDZANIE NT\SYSTEM		DEP
conhost.exe	64-bit	Poziom obowiązkowości – system	ZARZĄDZANIE NT\SYSTEM	ASLR	DEP (permanent)

- W00t ?
  - BinScope showed lack of DEP ?!?
- Bug in ProcessExplorer
- DEP is indeed forced on x64 arch. , but only for 64bit processes.

Exploitation strategy

- Trigger the vulnerability via xdmp:pdf-convert API.
- Convert binary does not drop privilages == auto priv escal
- convert
  - created by MarkLogic
  - lack of ASLR
  - Lack of DEP !!!
- Exploitation like in 90' – JMP ESP
- Remote Shell!

- Full exploitation write-up:
- http://blog.talosintelligence.com/2017/09/deep-dive-marklogic-exploitation.html

„Deep Dive in MarkLogic Exploitation Process via Argus PDF Converter”

MarkLogic 0wn3d via Iceni Argus PDF

VIDEO

Conclusions

Conclusions

- What kind of problems we could observe related with components :
  - misuse can increase vectors of attack
  - lack of support for basic mitigations in 2016!!!
    - even in big commercial solutions
  - Components inception
    - One component to rule them all!

Thank You!
Q&A

TALOS™

talosintelligence.com
blog.talosintel.com
@talossecurity

CISCO™