

TALOS™

Marcin 'Icwall' Noga
<http://www.icewall.pl>
@_Icwall

PWNing Warszawa 2017





When Third-party components become a source of all evil



Wstęp

- 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

- Jak komponenty dostarczone/udostępnione przez innych dostawców mogą wpłynąć na twój produkt.
- Przykłady braków, bugów, błędnego wykorzystania i nnych problemów użycia bibliotek w Enterprise'owych rozwiązaniach oraz ich konsekwencji.
- Analiza bugów
- Exploitacja
- Wnioski



Libarchive vs Splunk



Libarchive

- Opis
 - Bogata biblioteka pozwalająca odczytywać jak i tworzyć wiele różnych typów archiwów
- Motywacja
 - Duża ilość obsługiwanych formatów (ok. 20)
 - zip, rar, 7zip, mtree, cpio, xar, (...)
 - Popularność
 - Package Managers
 - Cmake
 - pkgutils
 - Archiving tools and File Browsers
 - Nautilus
 - Rozwiązania komercyjne
 - Splunk

Libarchive – Planowanie ataku

- Metoda wyszukiwania bugów
 - Sporo obsługiwanych formatów, opensource, podejźmy kompleksowo!
 - Fuzzing – na wielu maszynach
 - Automatic static code analysis
 - Code review

Libarchive - rezultaty

- 4 bugi
- Jaka metoda okazała się najskuteczniejsza ?
 - Fuzzing
 - LIBARCHIVE RAR **RESTARTMODEL** CODE EXECUTION VULNERABILITY
 - CVE-2016-4302
 - Automatyczna statyczna analiza kodu
 - 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 – analiza bugów

- LIBARCHIVE 7ZIP **READ_SUBSTREAMSINFO** CODE EXECUTION VULNERABILITY
 - Dlaczego fuzzer tego nie znalazł ?

```
Line 2164      ss->unpack_streams = unpack_streams;
Line 2165      if (unpack_streams) {
Line 2166          ss->unpackSizes = calloc(unpack_streams, // <----- ALLOCATION BASED ON OVERFLOWED INT
Line 2167                                     sizeof(*ss->unpackSizes));
Line 2168      Line 2134      uint64_t *usizes;
Line 2169      Line 2177      usizes = ss->unpackSizes;
Line 2170      Line 2178      for (i = 0; i < numFolders; i++) {
Line 2171      Line 2179          unsigned pack;
Line 2172      Line 2180          uint64_t sum;
Line 2173      Line 2181
Line 2174      Line 2182          if (f[i].numUnpackStreams == 0)
Line 2175      Line 2183              continue;
Line 2152      Line 2184
Line 2153      Line 2185          sum = 0;
Line 2154      Line 2186          if (type == kSize) {
Line 2155      Line 2187              for (pack = 1; pack < f[i].numUnpackStreams; pack++) {
Line 2156      Line 2188                  if (parse_7zip_uint64(a, usizes) < 0) // <--- BUFFER OVERFLOW
Line 2157      Line 2189                      return (-1);
Line 2190                      sum += *usizes++;
Line 2191              }
Line 2192      }
```

LIBARCHIVE 7ZIP READ_SUBSTREAMSINFO

- 43 krotnie powtórzone
- Czy taki plik będzie bezpieczny?
- Niestety NIE ;(
- A więc ?
- Debugger

ten sposób strigerować

	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	7z4'....,e'....
0010h:	00	00	00	00	70	04	00	00	00	00	00	00	58	FF	6C	6A	...p.....Xylj
0020h:	B9	0D	88	D0	AC	2D	6B	A3	5A	BB	E5	35	DF	D1	41	D9	..D--kZwâSbNAU
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	0B	00	01	24	06	F1	07	01	0A	53	07	D9+...\$.ñ...S.Ü
0070h:	64	6D	64	9A	BF	0E	D5	01	24	06	F1	07	01	0A	53	07	dmcd\$ç.ö.\$.ñ...S.
0080h:	D9	64	6D	64	9A	BF	0E	D5	01	24	06	F1	07	01	0A	53	Üdmcd\$ç.ö.\$.ñ...S
0090h:	07	D9	64	6D	64	9A	BF	0E	D5	01	24	06	F1	07	01	0A	.Üdmcd\$ç.ö.\$.ñ...
00A0h:	53	07	D9	64	6D	64	9A	BF	0E	D5	01	24	06	F1	07	01	S.Üdmcd\$ç.ö.\$.ñ...
00B0h:	0A	53	07	D9	64	6D	64	9A	BF	0E	D5	01	24	06	F1	07	.S.Üdmcd\$ç.ö.\$.ñ...
00C0h:	01	0A	53	07	D9	64	6D	64	9A	BF	0E	D5	01	24	06	F1	..S.Üdmcd\$ç.ö.\$.ñ
00D0h:	07	01	0A	53	07	D9	64	6D	64	9A	BF	0E	D5	01	24	06	..S.Üdmcd\$ç.ö.\$.
00E0h:	F1	07	01	0A	53	07	D9	64	6D	64	9A	BF	0E	D5	01	24	ñ...S.Üdmcd\$ç.ö.\$
00F0h:	06	F1	07	01	0A	53	07	D9	64	6D	64	9A	BF	0E	D5	01	.ñ...S.Üdmcd\$ç.ö.
0100h:	24	06	F1	07	01	0A	53	07	D9	64	6D	64	9A	BF	0E	D5	\$.ñ...S.Üdmcd\$ç.ö
0110h:	01	24	06	F1	07	01	0A	53	07	D9	64	6D	64	9A	BF	0E	.\$.ñ...S.Üdmcd\$ç.
0310h:	06	F1	07	01	0A	53	07	D9	64	6D	64	9A	BF	0E	D5	01	.ñ...S.Üdmcd\$ç.ö.
0320h:	24	06	F1	07	01	0A	53	07	D9	64	6D	64	9A	BF	0E	D5	\$.ñ...S.Üdmcd\$ç.ö
0330h:	01	24	06	F1	07	01	0A	53	07	D9	64	6D	64	9A	BF	0E	\$.ñ...S.Üdmcd\$ç.
0340h:	D5	0C	11	11	11	11	11	11	11	11	11	11	11	11	11	11	Ö.....
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.äö.ð.äö.ð.äö.ð
0380h:	00	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	00	.äö.ð.äö.ð.äö.ð.
0390h:	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	äö.ð.äö.ð.äö.ð.ä
03A0h:	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	ö.ð.äö.ð.äö.ð.äö
03B0h:	05	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	05	.ð.äö.ð.äö.ð.äö.
03C0h:	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	ð.äö.ð.äö.ð.äö.ð
03D0h:	00	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	00	.äö.ð.äö.ð.äö.ð.
03E0h:	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	äö.ð.äö.ð.äö.ð.ä
03F0h:	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	ö.ð.äö.ð.äö.ð.äö
0400h:	05	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	05	.ð.äö.ð.äö.ð.äö.
0410h:	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	ð.äö.ð.äö.ð.äö.ð
0420h:	00	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	00	.äö.ð.äö.ð.äö.ð.
0430h:	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	F5	05	F0	00	E1	äö.ð.äö.ð.äö.ð.ä
0440h:	F5	05	F0	01	16	A9	05	09	41	41	41	41	41	41	41	41	ö.ö.ö.AAAAAAAAA
0450h:	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAA
0460h:	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAA
0470h:	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAA
0480h:	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAA

PAYLOAD

TALOS

Libarchive vs Splunk

- Splunk?
 - „Umożliwia agregowanie logów z wielu źródeł, formatów oraz ich analizę”
- Jak odkryłem, że Splunk korzysta z libarchive?
 - Ogólne HINT’y
 - Google za specyficznym stringiem z pliku COPYING, COPYRIGHTS, LICENSE
 - tutaj jest to np. : „Copyright by Tim Kientzle”
 - lub ogólniej „Third-party software NazwaKomponentu”

Libarchive vs Splunk

splunk > docs PRODUCTS ▾ SOLUTIONS ▾ CUSTOMERS ▾ COMMUNITY ▾ SPLEXICON

Splunk® Enterprise
Release Notes
[Download manual as PDF](#)

Hide Contents ▴

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

Documentation / Splunk® Enterprise / Release Notes / Libarchive
[Download topic as PDF](#)
Libarchive
Version 3.2.2
The libarchive distribution as a whole is Copyright by Tim Kientzle and is sub...
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`

TALOS

Libarchive vs Splunk

- Udało się znaleźć potencjalne 2 wektory
 - archiwum w katalogu z logami
 - domyślnie tylko zip
 - upload pliku kmz (zip) w panelu webowym Splunk'a
- Gdzie dokładnie wykorzystane jest libarchive ? Jak striggerować bug'a ?
 - hackers-grep
 - `hackers-grep.py -n c:\splunk *.*.exe "archive_read_open"`
 - `splunkd.exe`

Splunk suicide

- Libarchive pozwala na aktywowanie wsparcia dla wybranych formatów lub wszystkich dostępnych
- Twórcy Splunka wybrali tę drugą opcję == możliwość obejścia ograniczeń z pliku konfiguracyjnego

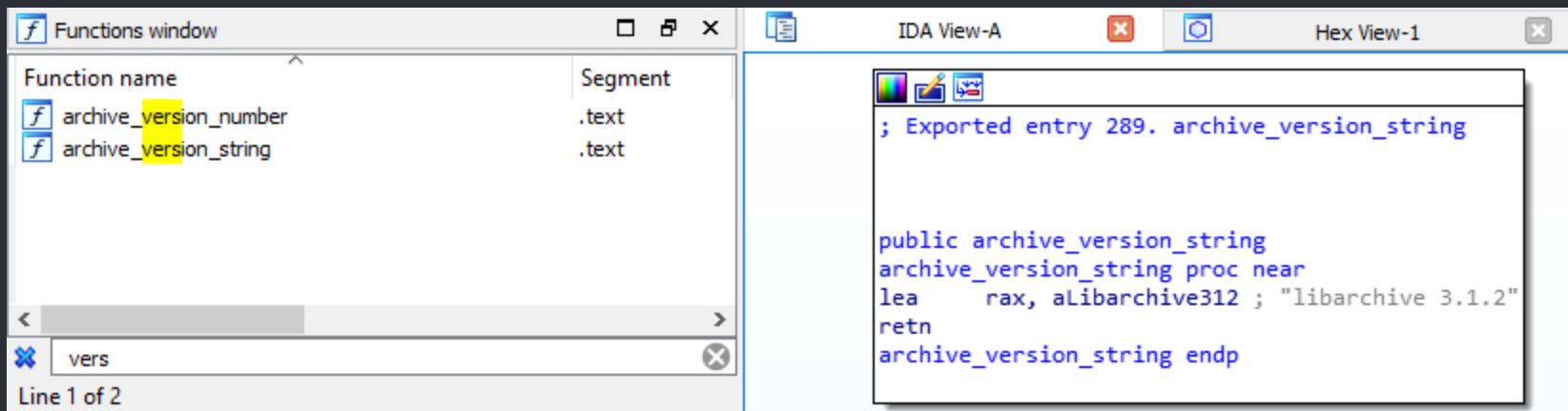
```
struct archive *a;  
a = archive_read_new();  
  
if( strcmp("7zip",formatName) == 0 ) { archive_read_support_format_7zip(a); }  
if( strcmp("cab",formatName) == 0 ) { archive_read_support_format_cab(a); }  
if( strcmp("rar",formatName) == 0 ) { archive_read_support_format_rar(a); }  
if( strcmp("iso9660",formatName) == 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);
```

Jakiej wersji libarchive używał Splunk?

- Libarchive w Splunku występuje jako : archive.dll



Od kiedy funkcjonuje ta wersja ?

- Testy wykonane ~ Czerwca 2016
- Splunk ver : 6.4.1
- Libarchive ver : 3.1.2
 - Wersja dostępna od Stycznia 2013 do Kwietnia 2016 !!!



Multi-format archive and compression library

The source distribution includes the libarchive library, the bsdtar and bsdcpio command-line programs, full test suite, and documentation:

- Stable release: [libarchive-3.1.2.tar.gz](#) [libarchive-3.1.2.zip](#) (since Jan 13, 2013)
- Legacy release: [libarchive-2.8.5.zip](#) (since Sept 3, 2011)



Multi-format archive and compression library

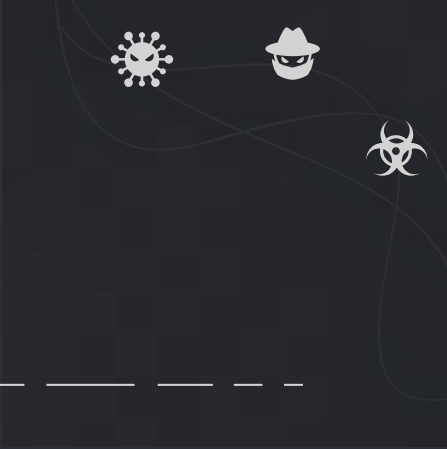
The source distribution includes the libarchive library, the bsdtar and bsdcpio command-line programs, full test suite, and documentation:

- Testing release: [libarchive-3.1.901a.tar.gz](#) (since Apr 10, 2016)
- Stable release: [libarchive-3.1.2.tar.gz](#) [libarchive-3.1.2.zip](#) (since Jan 13, 2013)
- [Legacy releases](#)

Splunk video

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

[PLAY](#)



MarkLogic vs „Converters”



W poszukiwaniu celu

- Google „metadata extraction”
- Trafiłem na stronę dokumentacji produktu MarkLogic

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.

- List obsługiwanych formatów
 - Presentation
 - Raster Image
 - Spreadsheet
 - Archives
 - Word Processing and General Office
 - (...)

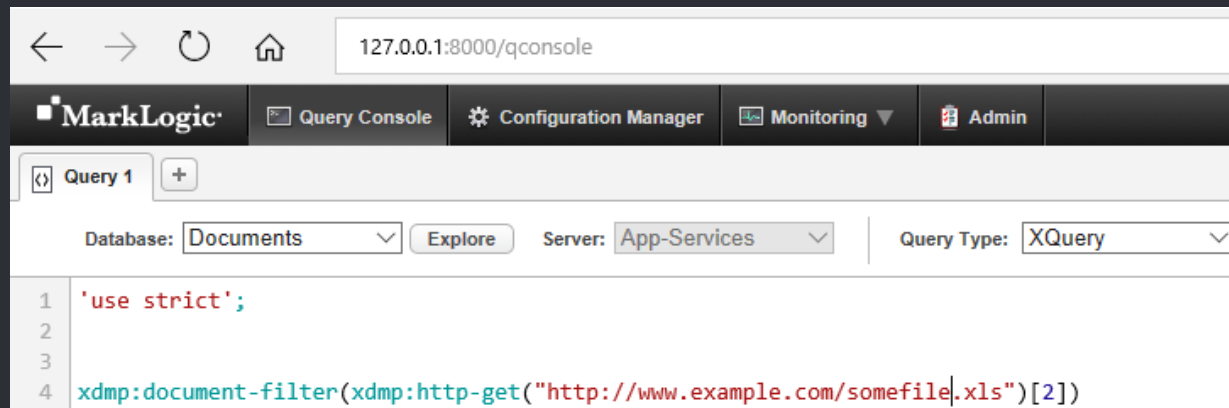
MarkLogic

- Opis
 - Baza NoSQL – nie relacyjna baza danych, nastawienie na agregowanie dużych ilości różnych danych (BigData)
- Czym jest BigData?
 - „olbrzymie” zbiory różnorodnych danych, których przetwarzanie (analiza/PARSOWANIE) może dostarczyć wartościowych informacji.
- Lista klientów
 - <http://www.marklogic.com/customers/>



Gdzie następuje ekstrakcja metadanych ?

- Wywołanie xdmf:document-filter na przykładowym pliku

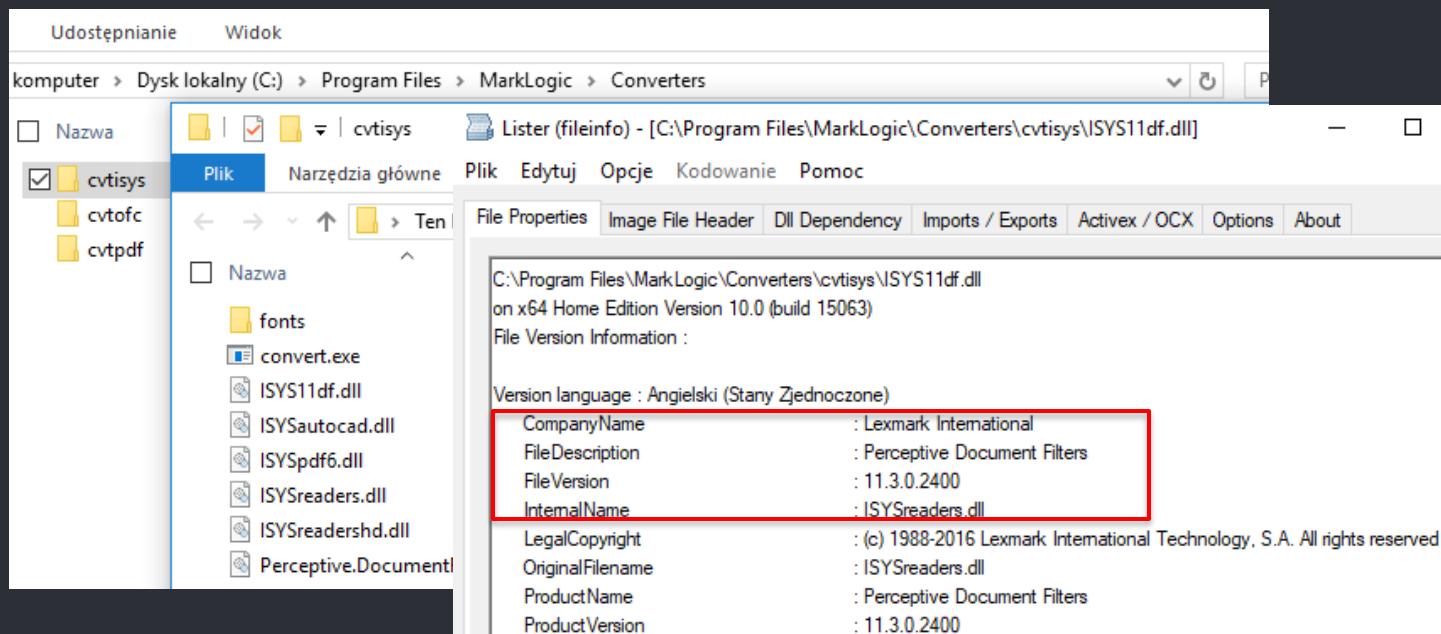


- Process Monitor

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

A więc konwertery

- 3 konwertery
- Google : nazwy plików, nazwa produktu (resource directory)

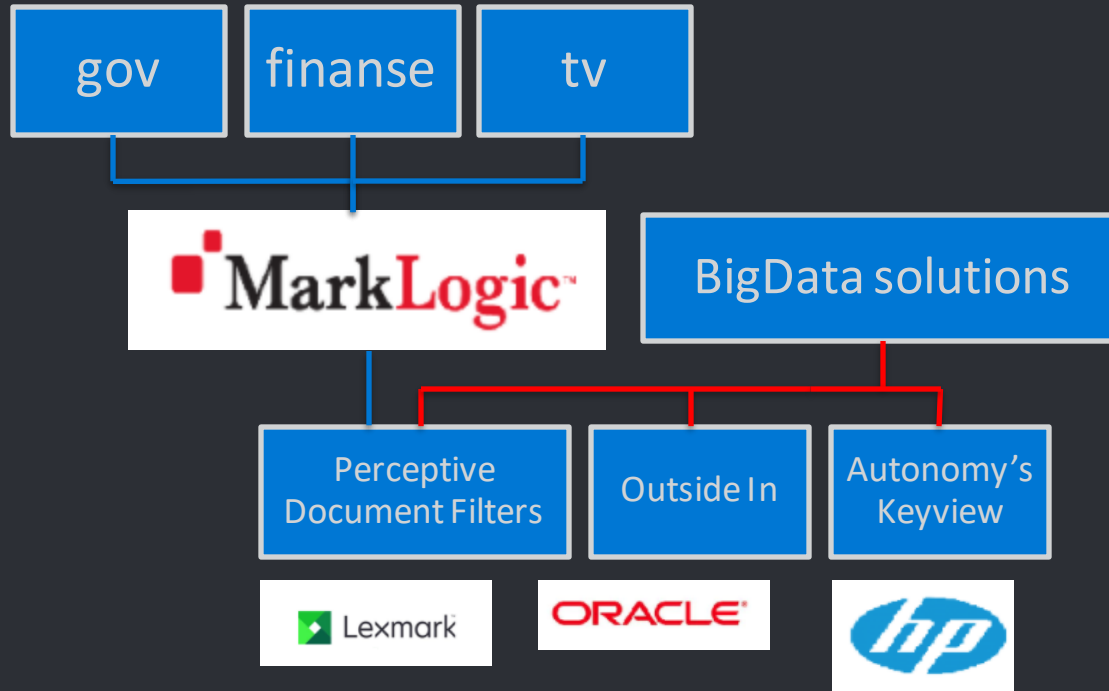


Perceptive Document Filters

- Opis
 - Właściciel
 - Lexmark
 - Zbiór bibliotek umożliwiający :
 - Identyfikacje typu pliku
 - Ekstrakcje tekstu i metadanych
 - Dekompresje archiwów
 - (...)
 - ~ 100 obsługiwanych formatów
 - Komercyjny
 - Close source

BigData

- Trzech głównych graczy
 - Oprogramowanie w postaci SDK (biblioteki,...)



Odnalezione bugi

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

Perceptive Document Filters - rezultaty

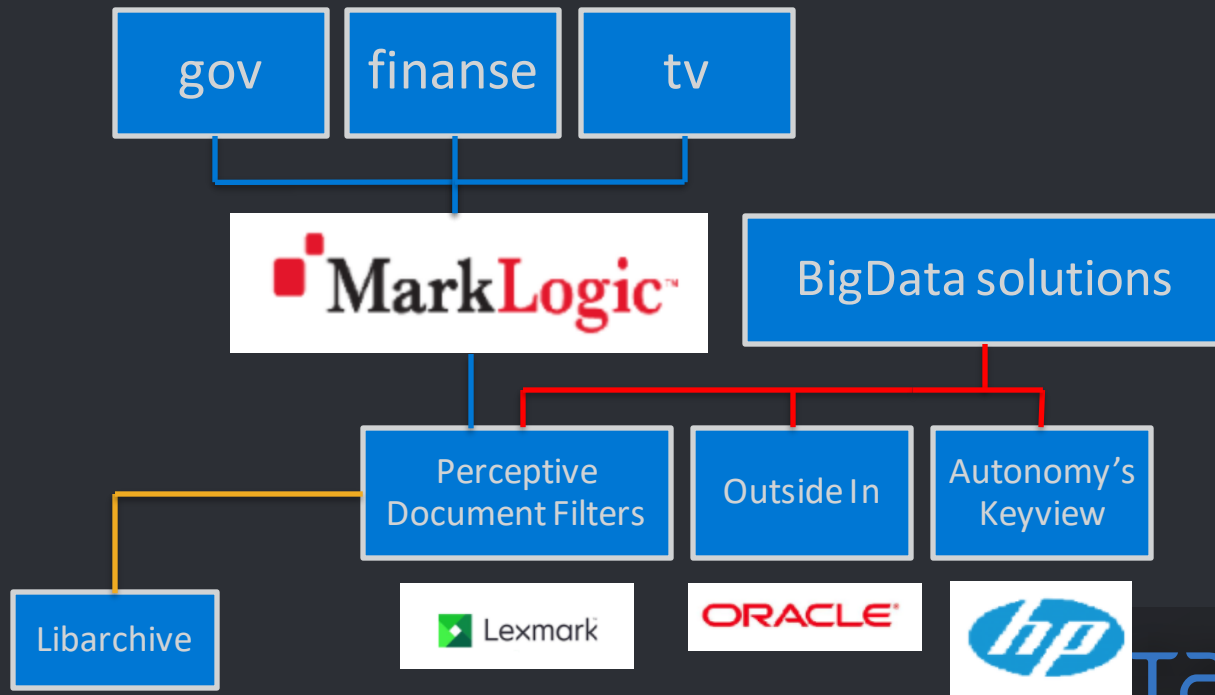
- 6 bugów

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 LibSYSpdf 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

- Metoda wyszukiwania bugów
 - Fuzzing / cross fuzzing
 - Gotowa aplikacja pod fuzzing – convert args
 - Głównie pliki office : xls, ppt, doc
 - wstępnie również pliki archiwów (korpus z libarchive), ale ...

Incepcja w bibliotekach

- Pierwszy crash w Perceptive Doc. Filters ujawnił, że biblioteka do obsługi archiwów wykorzystuje Libarchive.
- Oczywiście dość starą wersję!



Perceptive Document Filters – analiza buga

- LexMark Perceptive Document Filters XLS Convert Code Execution Vulnerability
 - CVE-2016-4335
- Funkcja triggerująca bug
 - reader::escher::MsofbtDggContainer::Handle
- Biblioteka
 - libISYSreadershd.so
- Typ błędu
 - Stack Based Buffer Overflow

Perceptive Document Filters – analiza buga

```
Line 1 struct_al * reader::escher::MsofbtDggContainer::Handle(struct_al *a1, __int64 *a2,
```

00000F00 00 01 00 20 00 00 04 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
00000F50 03 02 04 00 12 80 04 FF 93 02 04 00 13 80 07
00000F60 03 02 04 00 00 80 00 FF 93 02 04 00 14 80 05
00000F70 FF 00 00 00 00 00 85 00 13 00 2E 13 00 00 00
00000F80 00 SIZE [DWORD] 2 65 60 PAYLOAD [SIZE] C 00
00000F90 04 00 01 00 01 00 C1 01 00 00 00 00 00 00 00 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

Line 10 }
Line 11 if (recType == 0xF016u)
Line 12 {
Line 13 CPageMemoryStream::Read(&localBuffer, MSOFBH_header->size)
Line 14 }

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 OfficeArtFdgBlock
remainingData 03 08 16 F0 00 03 00 00 81 00 0x00000fce 0x0000085a DataItem_UByteArray



Exploitacja

CVE-2016-4335



W momencie odpalenia xdmf:document-filter

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

Proces **convert** uruchomiony z uprawnieniami **daemon**.

Sprawdzenie mitigacji w Perceptive Doc. Filters

```
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

Strategia eksploatacji

- Strigerowanie buga poprzez odpalenie xdmf:document-filter API.
- Binarka convert nie zrzuca uprawnień == auto priv escal
- Convert
 - binarka napisana przez MarkLogic
 - brak ASLR'a
- ROP (DEP bypass)
- Remote Shell!

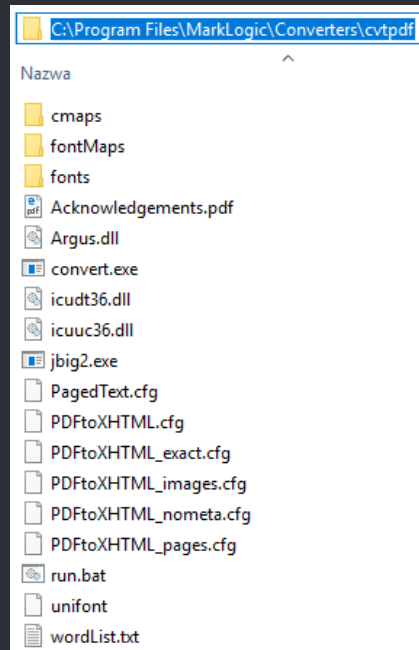
- Pełny opis procesu eksploatacji:
- <http://blog.talosintelligence.com/2017/06/lexmark-perceptive-vuln-deep-dive.html>
„ Deep dive in Lexmark Perceptive Document Filters Exploitation”

MarkLogic Own3d via Perceptive Doc. Filters

[VIDEO](#)

Iceni Argus PDF

- Opis
 - Właściciel
 - Iceni
 - Komercyjny
 - Close source
 - Przeznaczenie w MarkLogic
 - Ekstrakcja kontentu z PDF
 - Konwersja PDF do XHTML
 - Sposób wywołania w MarkLogic
 - xdm:pdf-convert



Iceni Argus PDF – rezultaty fuzzowania

- 10 bugów

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 – analiza buga

- Iceni Argus ipfSetColourStroke Code Execution Vulnerability
 - **CVE-2016-8333**
- Funkcja triggerująca bug
 - ipNameAdd
- Typ błędu
 - Stack Based Buffer Overflow
- Biblioteka
 - Argus.dll/so

Iceni Argus PDF – analiza buga

```
Line 1 int __cdecl ipNameAdd(char *src)
Line 2 {
Line 3     int v1; // esi@1
Line 4     int result; // eax@2
Line 5     int v3; // eax@5
Line 6     int v4; // esi@7
Line 7     char v5; // [esp+Ch] [ebp-11Ch]@1
Line 8     char dest[255]; // [esp+18h] [ebp-110h]@1
Line 9     int v7; // [esp+118h] [ebp-10h]@1
Line 10
Line 11     v7 = *MK_FP(__GS__, 20);
Line 12     strcpy(dest, src);
Line 13     v1 = rbtree_lookup(&v5, ipd[365]);
Line 14     if ( strlen(src) > 0xFF )
Line 15     {
Line 16         v3 = ipGStrGetStr("ipnametree.c", 0, "Name too long");
Line 17         icnErrorSet(28, v3);
Line 18         result = 0;
Line 19     }
```

too long '%s'");



Exploitacja

CVE-2016-8333



Może tym razem na Window'e ?

- Sprawdzenie używanych mitigacji
 - Rezultat z 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)

- Ale jak to ?
 - BinScope pokazywał brak DEP'a ?!?
- Błąd w ProcessExplorer'e
- DEP wymuszony na x64, ale tylko dla x64bit procesów

Strategia eksploatacji

- Strigerowanie buga poprzez odpalenie xdmf:pdf-convert API.
 - Binarka convert nie zrzuca uprawnień == auto priv escal
 - convert
 - binarka napisana przez MarkLogic
 - brak ASLR'a
 - brak DEP
 - Remote Shell!
 - Pełny opis procesu eksploatacji:
 - <http://blog.talosintelligence.com/2017/09/deep-dive-marklogic-exploitation.html>
- „Deep Dive in MarkLogic Exploitation Process via Argus PDF Converter”

MarkLogic Own3d via Icenii Argus PDF

[VIDEO](#)



Wnioski



Wnioski

- Zaobserwowane problemy związane z komponentami:
 - błędne wykorzystanie powoduje zwiększenie wektora ataku
 - brak wsparcia/implementacji podstawowych mitigacji w 2016 roku!!!
 - nawet w dużych komercyjnych rozwiązaniach
 - problematyczny „support” – rzadkie releasy lub ich brak
 - konieczność obserwacji wersji dev.
 - One component to rule them all!
 - wykorzystywanie komponentu, który od dawna jest już nie rozwijany!



Dziękuję!
Q&A



TALOS™

talosintelligence.com

blog.talosintel.com

[@talossecurity](https://twitter.com/talossecurity)

