

Hashes:

PO-SCSP24090838.docx:

897ee7659b61315c82b5d89f9a7d4297f2840b54da61efb9ae543f35e2517f63

Austria.rtf: a2987f63f96d725c2e95d3133a150716208382f06abedd07b93c4249374d82cf

AdobeID.pdf: 447fdc076abf331b88f87809ee194cd1c3634d0556339c9711d61adcdc2c01cf

Austria.rtf.bin: 2a2dc8f2ce00edf7cfecbeb4affd36833e300c42df27a9495c5daf70a4c6537c

CVE attempted to Exploit:

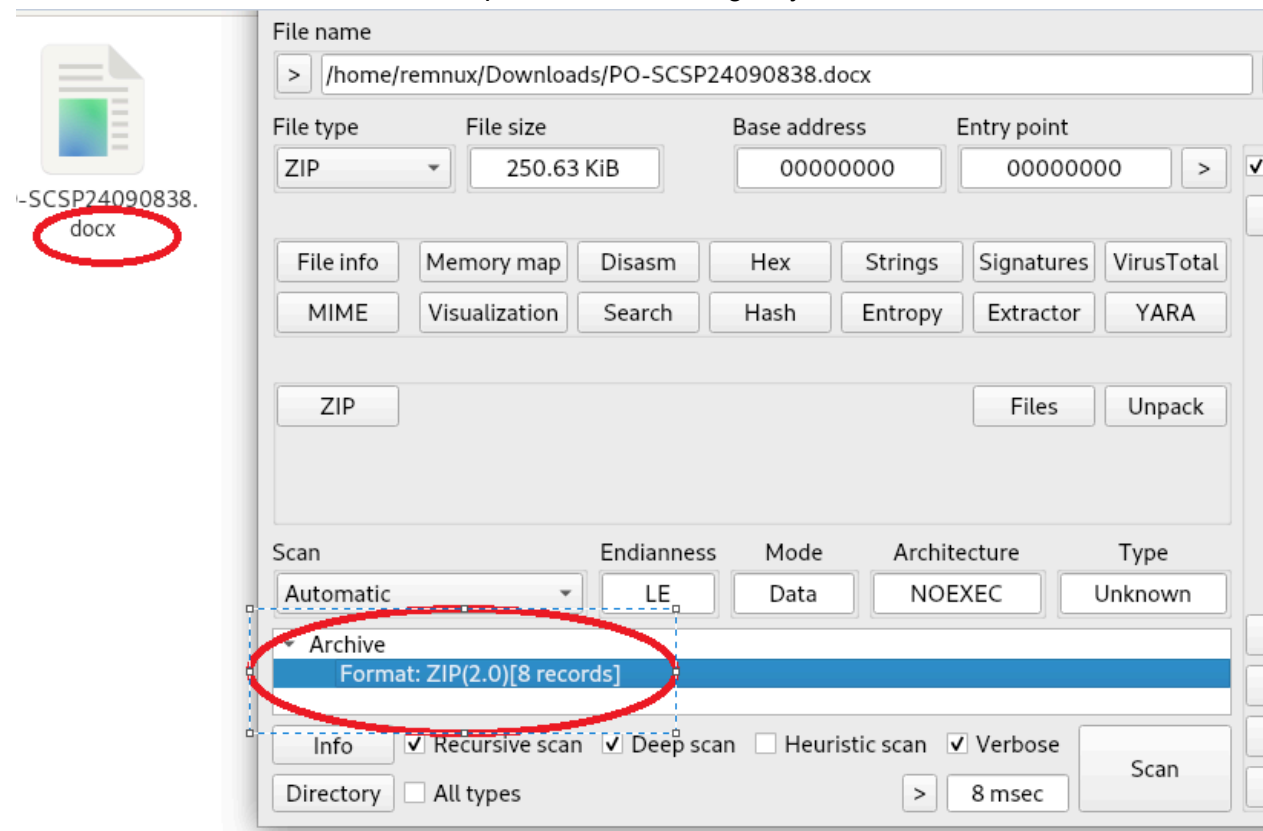
CVE-2023-36884

CVE 2018-0802

CVE 2017-1882

Information on Binaries

Fake docx extension. Identified as zip based on the magic bytes



Hex

Offset	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f	Symbols
0000:0000	50 4b 03 04 14 00 00 00 00 00 bb 6a 38 5a 00 00	PK.....j8Z..
0000:0010	00 00 00 00 00 00 00 00 00 00 06 00 00 00 5f 72_r
0000:0020	65 6c 73 2f 50 4b 03 04 14 00 00 00 00 00 33 01	els/PK.....3.
0000:0030	4a 5a 00 00 00 00 00 00 00 00 00 00 00 00 05 00	JZ.....
0000:0040	00 00 77 6f 72 64 2f 50 4b 03 04 14 00 00 00 08	..word/PK.....
0000:0050	00 e5 3d f1 56 e7 8a 3d 91 ef 00 00 00 af 01 00	..=.V..=.....
0000:0060	00 13 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79[Content_Ty
0000:0070	70 65 73 5d 2e 78 6d 6c 95 90 cd 4e c3 30 10 84	pes].xml...N.0..
0000:0080	5f c5 da 2b 4a 1c 38 20 84 92 f6 c0 cf 11 38 94	_..+J.88.
0000:0090	07 58 d9 9b c4 c2 7f f2 ba a5 7d 7b 36 2d 54 2a	.X.....}{6-T*
0000:00a0	e2 c2 d1 de 99 f9 76 a7 5f ef 83 57 3b 2a ec 52v._..W;*..R
0000:00b0	1c e0 ba ed 40 51 34 c9 ba 38 0d f0 be 79 6e ee@Q4...8...yn.
0000:00c0	40 71 c5 68 d1 a7 48 03 1c 88 61 bd ea 37 87 4c	@q.h..H...a...7.L
0000:00d0	ac c4 1b 79 80 b9 d6 7c af 35 9b 99 02 72 9b 32	...y... .5...r.2
0000:00e0	45 99 8c a9 04 ac f2 2c 93 ce 68 3e 70 22 7d d3	E.....,..h>p"}.
0000:00f0	75 b7 da a4 58 29 d6 a6 2e 19 b0 ea 1f 69 c4 ad	u...X).....i..
0000:0100	af ea 69 2f df a7 3d 0a 79 06 f5 70 12 2e ac 41	..i/..=.y..p...A
0000:0110	01 e6 ec 9d c1 2a 02 bd 8b f6 17 a6 f9 46 b4 62*.....F.b
0000:0120	3d 6a 78 76 99 af 44 00 fa 6f 44 1d 2f 09 17 80	=jxv..D...oD./...
0000:0130	65 2a be 57 69 a6 38 4b ea 0d 4b 7d c1 20 2a fd	e*.Wi.8K...K}. *
0000:0140	99 8a d5 36 99 6d 10 67 bb 00 fe b7 68 1a 47 67	...6.m.g....h.Gg
0000:0150	e8 1c b0 c4 e5 92 0c 31 4b e7 c1 b7 e7 49 40 171K....I@.

Selection:0000000000000000 Size:0000000000000002

OleID

Filename: P0-SCSP24090838.docx

Indicator	Value	Risk	Description
File format	Generic OpenXML file	info	
Container format	OpenXML	info	Container type
Encrypted	False	none	The file is not encrypted
VBA Macros	No	none	This file does not contain VBA macros.
XLM Macros	No	none	This file does not contain Excel 4/XLM macros.
External Relationships	0	none	External relationships such as remote templates, remote OLE objects, etc

remnux@remnux:~/Downloads\$

Unzip docx



Rtfobj Austria.rtf

```
=====
File: 'Austria.rtf' - size: 2945181 bytes
-----
id | index | OLE Object
-----
0 | 00003A12h | format_id: 2 (Embedded)
   |          | class name: b'Package'
   |          | data size: 482968
   |          | OLE Package object:
   |          | Filename: 'AdobeID.pdf'
   |          | Source path: 'C:\\Path\\AdobeID.pdf'
   |          | Temp path = 'C:\\Path\\AdobeID.pdf'
   |          | MD5 = 'b3dd9f55fbd3ecbb5b8831102cf9d4c2'
   |          | File Type: Windows PE Executable or DLL
-----
1 | 001012E8h | format_id: 2 (Embedded)
   |          | class name: b'Equation.3'
   |          | data size: 3072
   |          | MD5 = '403344b66690885723c6bf13bdc24fe9'
   |          | CLSID: 20E02C00-0000-0000-0C00-000000000004
   |          | unknown CLSID (please report at
   |          | https://github.com/decalage2/oletools/issues)
   |          | Possibly an exploit for the Equation Editor vulnerability
   |          | (VU#421280, CVE-2017-11882)
-----
remnux@remnux:~/Downloads/P0-SCSP24090838.docx.2/word$
```

Rtfobj -s 0 Austria.rtf and rtfobj -s 1 Austria.rtf



Austria.rtf



Austria.rtf_AdoBeID.pdf



Austria.rtf_object_001012E8.bin

.Pdf payload is executable

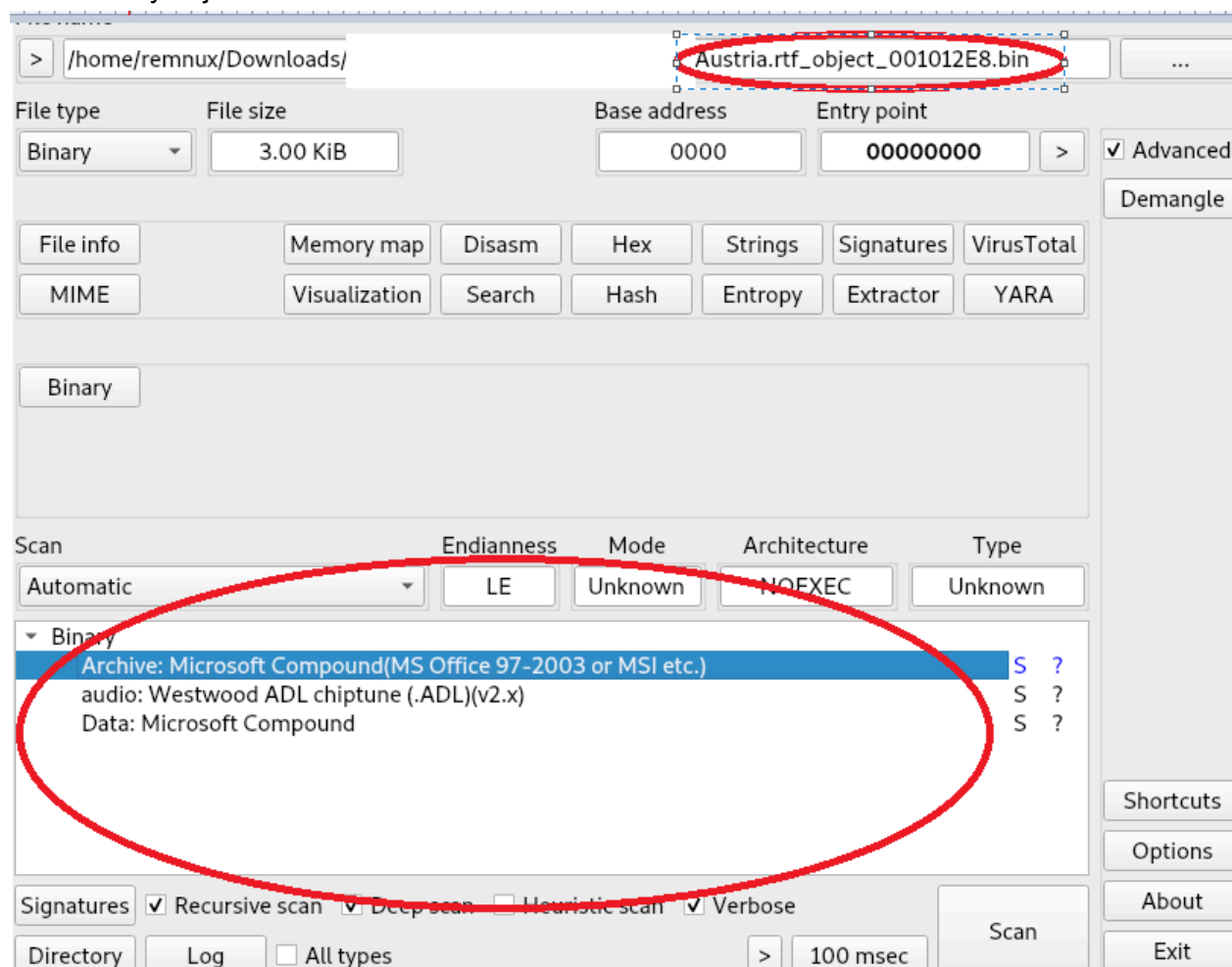
File name: /home/remnux/Downloads/word/Austria.rtf_AdoBeID.pdf

PE

Hex

Offset	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	Symbol
0000:0000	4d	5a	00	00	00	00	00	00	00	00	00	00	00	00	00	00	MZ...
0000:0010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000:0020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000:0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	78	00x...
0000:0040	0e	1f	ba	0e	00	b4	09	cd	21	b8	01	4c	cd	21	54	68!..L.!Th
0000:0050	69	73	20	70	72	6f	67	72	61	6d	20	63	61	6e	6e	6f	is program canno
0000:0060	74	20	62	65	20	72	75	6e	20	69	6e	20	44	4f	53	20	t be run in DOS
0000:0070	6d	6f	64	65	2e	24	00	00	50	45	00	00	64	86	02	00	mode.\$..PE..d...
0000:0080	00	00	00	00	00	00	00	00	00	00	00	00	f0	00	42	20B

Other binary object is a .ADL file?



[illegible]