#### Fixing Bugs in Binaries

#### Luis Miras Imiras <o> gmail.com

#### Agenda



- Introduction
- Feasibility of binary fixes
- Current third party patches
- Strategy
- Working Example
- Future of third party patches
- Questions

#### Introduction



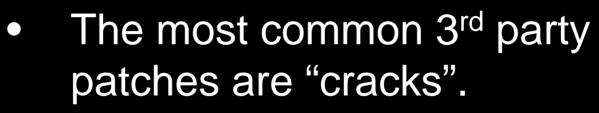
- Is the src available?
- What dependencies do we have?

# Don't wait for a vendor to get around to it, fix vendor bugs yourself!

## Feasibility of binary fixes

- Consider !/\$
- Complexity of fix relative to the bug.
- Fixing an "off by one" is easy
- Adding class members can get complicated.

#### **Current third party patches**



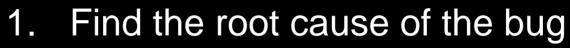
- Ilfak's WMF patch
  - Determina's and Eeye's CreateTextRange() patch



## Mantra : "least amount of change that gets the job done"



## Strategy



- 2. Locate the problem code in disassembly
- 3. Make a fix
- 4. Test, test, and test
- 5. Refine/Refactor the fix
- 6. Test, test, and test

## Applying fixes



Patching the file on disk/storage Patching at runtime. – injecting code, dll, hooks, etc.

Hybrid – Loaders (packers)

#### **Working Example**

#### Verizon xv6700





#### xv6700 specs

ightarrow



- Windows Mobile 2005
- 416Mhz pxa270 ARM Processor
  - 1.3 Mega pixel Camera
- EVDO
- WIFI
- Bluetooth
- USB ActiveSync Access

#### WM2005 Intro



- Part of the WinCE 5.0 familyWinCE 5.0
- Windows Mobile 2005 Pocket PC
- Windows Mobile 2005 Smartphone
- Windows Mobile 2005 Pocket PC
   with Phone

#### WM2005 Intro



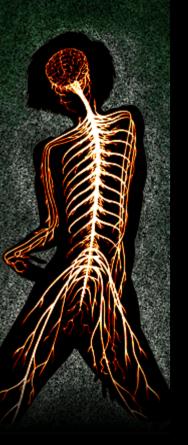
- Little Endian
- Very close to Win32
- Portable Executables
  - Same style hooking
- Debugging with VS2005 and IDA ARM debugger

## The Bug



- Reported on forums, pictures can't be mailed through Gmail pop3.
- Google is performing file validation.
- JPEG corruption

#### Virtual G – PPC imaging software







- Images opened and saved from Virtual G pass the Gmail test.
- File changes only in Exif section



#### JPEG and Exif use markers for data. ex. FFxx

SOI Marker	APP1 Marker	APP1 Data	Other Marker
FFD8	FFE1	SSSS 457869660000 TTTT	FFXX SSSS DDDD

E1 – Start of the Exif Header SSSS – Size field (includes 2 bytes for size field) 45786966 – ASCII for 'Exif'



CH I	원 Hex Workshop - [IMAGE_00001.jpg]																							
	Eile	Ed	t Ç	Qisk	Opt	tion	ns <u>T</u> oo	ols	Wind	low <u>H</u>	elp												-	Ξ×
1	s	<u>э</u> г	1 4	=7,	l v	F	. 8	5	C	8	8	r 🗈		5	- D D		0 E	n		(m)		- 10		
	7 3	î	96	₹	d0				2	1 K.	¢.	C)	16	10	0   B	S L	ŲF	0	Ľ×	) 🕀		· ]]	land (1)	
≤		~ <	$\sim$	>>	5	2	*	>>	^	3 1		<del>†∕_</del> +	- 4	ŧ	1 %	K [>]	At a	a↓ a≬	A	Q.	昭	昭	1%	*
11																			-					1
0	00	000	00	F	FD8	3 1	FFE1	0	0 <b>F</b> 9	457	8	6966	000	0	4949	2A00	· · · ·	E	xif		11*		-	~
0	00	000	10	1	1800		0000	0	800	OFO	1	0200	030	0	0000	4854					H	Г		
		000			300		1001		200		0	0000	6EO		0000	1A01	C			n.				_
		000			1500		0100	- T.	000			0000	1B0		0500	0100		u	• • •			•		
		000			1000		7D00		000		œ.,	0300	010		0000	0200	}.	(	• • •			•		
		000			0000		3201		200		- C	0000 6973	698		0000	3B01					•••	-		
		1000			1200		0400 9900		000	407		0000	417		0400 6163	0100		L						
		1000			048		0000		001		-	0048			0001	0000	н				acine	-		
		1000			032		3030	- <b>T</b>	63A		- C - C - C - C - C - C - C - C - C - C	3A30	372		3136	3A30	.200				16:1	5		
		000	0.0		AE O		3035		005			9002	001		0000	OODD	0:05							
0	00	000	во	0	000	)	0000	9	007	000	4	0000	003	0	3231	3009					210			
0	00	000	CO	9	203	3 1	0001	0	000	000	0	0000	000	2	A004	0001								
		000			1000		0800		200		- C	A004	000	_	0000	OOEO								
		1000			100	5 1	0000		000			0032	303		363A	3036					6:01			
		000			DEA		3720		136			303A	303		FFEO	0010		16:1			• • •	12		
1 1 -		1001			A46	2 8	4946		001	010		0001	000	-	0000	FFEO	JFIF					12		
		1001			872		4A46 DBOA		858			FFD8 OBOE	FFD		0043 0F13	000D 2015	.rJF	XX.	• • •	• • •	.c.	12		
		1001			312		1213		71C	1E1		202E	293		302E	2015 292D		;::	•••	11	 ο			
		001			2033	5 9	3A4A		100.00	364		372C	2D4		5741	464C	,3:J							
1 1 -		1001		_	E52		5352		23E			5A50	604	- T	5152	4FFF	NRSR							
		001			BOO	j .	4301		EOE	OE1		1113	261		1526	4F35	C.							
0	00	001	.70	2	2D35	5 .	4F 4F	4	F4F	4F4	F	4F4F	4F4	F	4F 4F	4F4F	-500	000	000	000	0000	)		
0	00	1001	80	4	F4F	۰.	4F 4F	4	F4F	4F4	F	4F4F	4F4	F	4F 4F	4F4F	0000							
0	00	001	.90	4	F4F		4F 4F	4	F4F	4F4	F	4F 4F	4F4	F	4F 4F	4F 4F	0000					)		
1 1 -		1001			F4F		4F 4F				-	0800	780		A003	0122	0000		• • •	х.	• • • '			
		001			0002		1101					DDOO			OAFF	C400		• • •	• • •	• • •	• • •	12		-
JU	UL	1001	.cu	11	FUU	1	1001	U	501	010	1	0101	010	U	0000	0000	• • • •	• • •	• • •	• • •	• • •	•2		~
100		MAGE	_00	0																				
×	itru	cture	Viev	ver	(exif.	hsl	)	-			-	_ 	+	X	Compare	Results			All	_			•	•
Πŕ	Ad	dress	/ Na	me								V.	alue	ī			S	ource				Count	t	
					ct EXI	E I	HDR																	
	10	00000	013	, ci ci	ee ena		ID IX					e e												
													- 11											
													- 11											
													- 11											
													- 11											
																			_					
	<	5	_		100			-		_	_		>		<	_	1111							>
11/	D	ata Ir	spe	cto	r As	5tr	ucture	e Vie	ewer	1				11	\ Compa	are { ⊂ł	hecksum	À Fir	nd )	Bo	okmar	ks λ	Out	put /
Read	ly .															Offset: 0	00000380	) (	Valu	e: 56	20			55: //
														1									-	



Image: Big Edit Disk Options Looks Window Help         Image: Big Edit Disk Options Looks Options Looks Options         Image: Big Edit Disk Options         Image: Big Edit Di	× → →     ← + → →     ≪   ≫
→ ~ « > 5 2 2 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	+ + →     + + →
000000000 FFD8 FFE1 00F9 4578 6966 0000 4949 2A00Exif.II*. 00000010 8800 0000 USUU 0F01 0200 0300 0000 4854HT 00000020 4300 1001 0200 0700 0000 6E00 0000 1A01CHT	8   <mark>%  </mark> #
00000010 0800 0000 0800 0F01 0200 0300 0000 4854HT 00000020 4300 1001 0200 0700 0000 6E00 0000 1A01 Cn	
00000010 0800 0000 0800 0F01 0200 0300 0000 4854HT 00000020 4300 1001 0200 0700 0000 6E00 0000 1A01 Cn	
00000020 4300 1001 0200 0700 0000 6E00 0000 1A01 Cn	<u>^</u>
1111111113111500 0100 0000 7500 0000 1801 0500 0100	
00000060 0200 0400 0000 4C75 6973 6987 0400 0100Luisi	
00000070 0000 9900 0000 0000 0000 4170 6163 6865Apache	
00000080 0048 0000 0001 0000 0048 0000 0001 0000 .HH	
00000090 0032 3030 363A 3036 3A30 3720 3136 3A30 .2006:06:07 16:0	
000000A0 303A 3035 0005 0003 9002 0014 0000 00DD 0:05	
000000B0 0000 0000 9007 0004 0000 0030 3231 30090210.	
000000C0 9203 0001 0000 0000 0000 0002 A004 0001	
000000D0 0000 0060 0200 0003 A004 0001 0000 00E0	
000000E0 0100 0000 0000 0002 3030 363A 30362006:06	
000000F0 3A30 3720 3136 3A30 303A 3035 FFE0 0010 :07 16:00:05	
00000100 4A46 4946 0001 0100 0001 0001 0000 FFE0 JFIF	
00000110 0872 4A46 5858 0010 FFD8 FFDB 0043 000D .rJFXXC	
00000120 090A 0B0A 080D 0B0A 0B0E 0E0D 0F13 2015	
00000130 1312 1213 271C 1E17 202E 2931 302E 292D')10.)- 00000140 2C33 3A4A 3E33 3646 372C 2D40 5741 464C .3:J>36F7@WAFL	
00000140 2C33 3A4A 3E33 3646 372C 2D40 5741 464C .3:J>36F7@WAFL 00000150 4E52 5352 323E 5A61 5A50 604A 5152 4FFF NRSR2>ZaZP`JQR0.	
00000160 DB00 4301 0E0E 0E13 1113 2615 1526 4F35C&&05	
00000170 2D35 4F4F 4F4F 4F4F 4F4F 4F4F 4F4F 4F4F 4F	
00000180 4F4F 4F4F 4F4F 4F4F 4F4F 4F4F 4F4F 4F	
00000190 4F4F 4F4F 4F4F 4F4F 4F4F 4F4F 4F4F 4F	
000001A0 4F4F 4F4F FFC0 0011 0800 7800 A003 0122 0000	
000001B0 0002 1101 0311 01FF DD00 0400 0AFF C400	
000001C0 1F00 0001 0501 0101 0101 0100 0000 000	
() IMAGE_000	
Structure Viewer (exif.hsl)	• 4
	Count
Address / Name Value	
	>
	s 👌 Output 🖊
Ready Offset: 0000038D Value: 5620	55: //



K	He	×W	ork	sho	p - [l	MA	GE_0	0001.	ipg]											
107	) Eil	eΕ	dit	Dis	< Opt	ions	Too	ols <u>W</u> in	dow <u>H</u> elp	>										- 8 ×
	£.	<u> </u>		5	1 ×		8	22	88	+ (B)	1	10	B	S L	0 F		Ŧ2 (Ŧ		n llha	
1				2				panalier panaerro		+=				9 5	4 1	• 11	20	,    ==	<u> </u>	
	≒	~	<<	<b>&gt;&gt;</b>	52	2	≦ ≥	3 ^	3 1	* +		*	1 %	[ ]	A† a	↓ a‡A	Ų.	) 'B'	昭 :	% 🐲
Ľ.								-									111			
		000			FD8	F	FE1	00F9	4578	6966	000		4949	2A00		.Exi	f	II*	-	^
1.1.1		000	2.7	201	3800		000		OF01				0000	4854				H	Г	
		000			4300		001	0200		0000	6EO	100	0000	1A01	C		n.			
		200			0500	1.1	100	0000		0000	180		0500	0100		.u.				
		000			0000		DOO	0000				100	0000	0200	}	. (			•12	
		000			0000		201	0200					0000	3B01					12	
		000			0200		400	0000		6973	698		0400	0100		.Lui				
		000			0000	1.0	900	0000				ST 11	6163	6865			Ap	ache	9	
1 3		000		2010	0048	199	000	0001	100000	0048	000	35 1	0001	0000	.H	100	H	::::		
		000			0032		030	363A		3A30	372		3136	3A30	.2008		:07	16:1	J	
		000			ACOE		035	0005		200.00	001		0000	OODD	0:05.				•	
		000 000			0000 9203		1.1.1	9007			003		3231 A004	3009				210	•	
		000		201	1000		001	0200			000		0000	0001 00E0					12	
		000			0100		000	0000			303		363A	3036			200	6:0		
		100	200	2.1	3A30		720	3136			303		FFEO	0010	:07 1	6:00			2	
1 3		000			4A46		946	0001					0000		JFIF.		1.00	•	ia.	
		000			3872		A46						0043	OOOD	.rJFX			· · · ·	18	
		000			090A			0800			OEO		0F13	2015	.1312	····			12	
		200			1312		213				293		302E	292D			1	<u>ο</u>	10	
1.1.1		000			2033			3E33				37 S	5741	464C	,3:J>					
		000			4E52			323E					5152	4FFF	NRSR2					
		000			DBOO		301				261		1526	4F35	C					
		000			2D35		F4F	4F4F			4F 4		4F4F	4F4F	-5000					
		000			4F4F		F4F	4F 4F		4F4F	4F4		4F4F	4F4F	00000					
		000			4F4F		F4F	4F 4F		4F 4F	4F 4		4F4F	4F4F	00000					
		000			4F4F			FFCC					A003	0122	0000.				u .	
1 3		000			0002	100	8 5 7 2		01FF				OAFF	C400				00000		
									0101										• 2	~
-	_	MAG			-															
		MAG	L_0	50	1															
×	Stru	uctur	e Vie	wer	(exif.h	nsl)				- 	+	×	Iompare	Results		All				•
T	-	Idres	_							V	alue	ΠE			Sou	urce			Count	
	1.00				Jot EXIF	e pr	ne				}									
	Leafe	10000	1004	suru	JUL EVIL	r_nı	JK			ા	<i>f</i>									
	L .										- 11									
											- 11									
	L										- 11									
	<				100						>		<		IIII		E.			>
	1000	Data	Insp	ecto	EXAMPLE.	itru	cture	Viewer			0.000	1		re 🖉 🖯	hecksum	λ Find	λ Be	okmar	ks λ	Output /
Re	ady														0000038D		lue: 56		0	55:
	ωuγ	_	_											onsec. c		140		~-0		00.



Exif header is too large. "Off by one"

 Manually changing the size field passes the Gmail file check.

• The bug is identified!

#### **ARM assembly intro**



- RISC 32 bit
- Little/Big Endian
- 16 bit Thumb code
- Load/Store Architecture

http://blogs.msdn.com/windowsmobile/archive/200 5/05/10/ArmTutorial.aspx

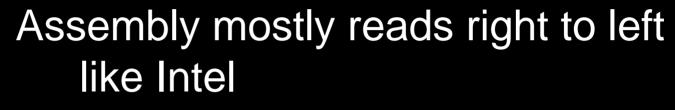
#### Registers



RO-R3 General, functions args R4-R11, R12 General SP Stack Pointer PC Program Counter LR Link Register



#### Instructions



mov reg, reg mov reg, #0x00

Idrb reg, address

strb reg, address

#### **Camera.exe Analysis**

- Copy it to PC using ActiveSync connection
- IDA identifies file as an ARM PE
  Flirt recognizes WinCE libs



#### **Bug in Disassembly**

- Need to locate the bug in disassembly
- Locate construction of Exif header
  "Exif" not found in strings list



#### **Bug in Disassembly**

 Look for individual letters being written out.
 mov register, #0x45 ; 'E' strb register, buffer

Success at function 0x05BCC0



#### **Bug in Disassembly**

R1, #0x45 ; E 0005BD38 MOV 0005BD3C STRB R1, [R2,#2] [ snip ] 0005BD58 MOV R0, #0x78 ; X R0, [R2] 0005BD5C STRB [snip] MOV R0, #0x69 ; i 0005BD78 0005BD7C STRB R0, [R2] [ snip ] 0005BD98 R0, #0x66 ; f MOV R0, [R2] 0005BD9C STRB

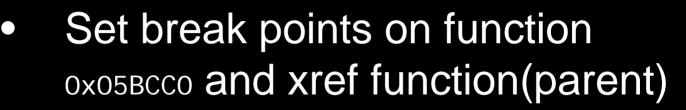
#### **Runtime Analysis**



- Combining runtime and static analysis speeds up the process
- Visual Studio 2005 debugger can connect to devices over ActiveSync

http://www.airscanner.com/security/WM5debugVS2005.pdf

#### **Runtime Analysis**



'E' gets written to a buffer identifying the location of size "Watch" for the size being written

#### **Runtime Analysis**



Size v	writing	iden	tified:
05BF7C			R3, #0xFF00
05BF80	ADD	R1,	RO, #OxFE
05BF84	MOV	R2,	R1, LSL#16
05BF88	MOV	RO,	R2, LSR#16
05BF8C	MOV	R1,	RO, LSR#8
05BF90	ADD	RO,	R3, #OxFE
05BF94	STRB	R1,	[R4] ; size write
05BF98	AND	R2,	R1, #OxFF
05BF9C	STRB	RO,	<pre>[R4,#1] ; size write</pre>

Fix



The fix can divert execution before the last write (lsb).

A branch is put in, but first space to put in code must be found.

#### Where to patch?

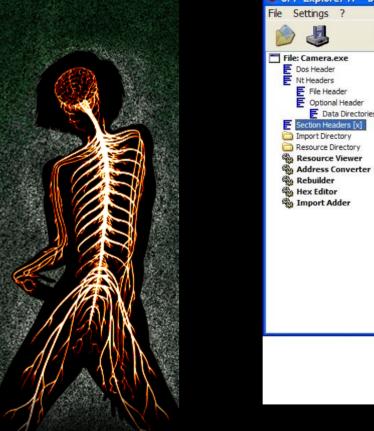


Code caves between functions
 Extending sections

• New sections



#### **Extending a Section**



	Name	Virtual Size	Virtual Ad	Raw Size	Raw Address	Relo
e: Camera.exe	Rvtel 81	Dword	Dword	Dword	Dword	Dwo
Dos Header Nt Headers	.text	(00089BB4)	00001000	00089000	00000400	000
File Header	CSC.	00000F3C	0008B000	00001000	0008A000	000
Optional Header	RszRotCs	00001AB8	0008C000	00001C00	0008B000	000
🔄 🛃 Data Directories [15]	Preview	00001B0C	0008F000	00001C00	0008CC00	000
Section Headers [x]	.rdata	00004760	00090000	00004800	0008F800	000
Import Directory Resource Directory	.data	0000D8FC	00095000	00008A00	00093000	000
Resource Viewer	.ndata	00002DE0	000A3000	00002F00	0009BA00	000
Address Converter	rsrc	00013A14	000A6000	00013C00	0009F800	00
a Hex Editor a Import Adder	<	10				

#### **Extending a Section**



.text section virtual size = 0x89BB4

.text section raw size = 0x89C00

Virtual size can be increased to 0x89C00 Producing 0x4C of extra space

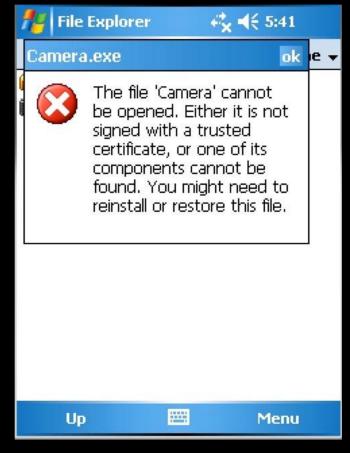
#### The Fix



05BFAC	ADD BL MOV	R1, R0, #0xFF R0, SP, #0x10+arg_4 sub_48400	MOV MOV MOV MOV	R9, R9 R9, R9 R9, R9
09ABC8 09ABCC 09ABD0 09ABD4	STRB AND ADD BL MOV	R11, [R4,#1] R1, R0, #0xFF R0, SP, #0x10+arg	_4	

#### Signed Code Error





# Signed Code Fix

Signed code is pointed to by the Security Data Directory in the PE header.

Set RVA and size to NULL.

### **Signed Code Fix**



#### 

File Settings ?	
-----------------	--

	Memher	Offset	Size	Value	^
	Export Directory RVA	00000180	Dword	0000000	
File: Camera.exe	Export Directory Size	00000184	Dword	0000000	
Dos Header	Import Directory RVA	00000188	Dword	00093628	
Nt Headers File Header	Imnort Directory Size	0000018C	Dword	00000168	
File Header	Resource Directory RVA	00000190	Dword	000A6000	
Data Directories [15]	Resource Directory Size	00000194	Dword	00013A14	
E Section Headers [x]	Exception Directory RVA	00000198	Dword	000A3000	
import Directory	Excention Directory Size	00000190	Dword	00002DE0	
Resource Directory     Resource Viewer	Security Directory RVA	000001A0	Dword	000B2400	
Address Converter	Security Directory Size	000001A4	Dword	00000370	
🐁 Rebuilder	Relocation Directory RVA	000001A8	Dword	0000000	
Hex Editor	Relocation Directory Size	000001AC	Dword	00000000	
import Adder 🖏	Debug Directory RVA	000001B0	Dword	00090000	
	Debug Directory Size	000001R4	Dword	0000001C	
	Architecture Directory RVA	000001B8	Dword	0000000	
	Architecture Directory Size	000001BC	Dword	00000000	
	Reserved	000001C0	Dword	0000000	
	Reserved	000001C4	Dword	00000000	
	TIS Directory RVA	000001C8	Dword	0000000	
	TLS Directory Size	00000100	Dword	00000000	
	Configuration Directory	000001D0	Dword	0000000	<b>~</b>

#### Results



H Hex Worl		-	_										
Eile Edi	t <u>D</u> isk	Optio	ns <u>T</u> o	ools <u>V</u>	Vindow	Help						- ć	X
🕞 🖬 🖬 🤅	3 %	h 6	2 2	\$ \$	•	1 1	o B	S L	QFI	1 😥	• 🗖	←	<del>(</del>
≒~ «	» 🗳 2	<u>&gt; ~ &gt;</u>	<u>} ~  </u>	&	<del>†∕</del> - +	- +	1 %	K] [>]	A↑ a↓	a A	<b>6</b> 8 8	2%	10 10 10
1										1.1.1			
00000000		FFE1			6966		4949	2A00	· · · · <u>-</u>	.Exif	II*.		^
00000010			0800		0200		0000	4854			HT		
00000020					0000	6E00	0000		C		n		
00000030		0100			0000		0500			.u			
00000040		7000	0000		0300		0000		}	. (			
00000050		3201		1400		8500	0000	3B01					
00000060		0400	0000				0400	0100		Luis.			
00000070			0000		0000		6163				Apache		
00000080		0000	0001	0000	0048	0000	0001	0000	.H				
00000090		3030	363A		3A31 9002		0000	3A31			8 06:1		
000000A0		0000	9007			0014	3231	00DD 3009	8:36.		0310		
000000000000000000000000000000000000000		0000	0000		0000	0002	A004	0001			.0210.		
000000000000000000000000000000000000000		00001	0200		A004	0002	0000	OOEO					
000000DC		0000	0000		0032	3030	363A	3036			006:06		
000000EC		3820	3036	3A31		3336	FFEO	0010	:18 00	6:18:			
00000100	10000	4946	0001	0100	0001	0001		FFEO	JFIF.		30		
00000110		4A46			FFD8		0043	OOOD	.JFX				
00000120		OBOA					0F13	2015	Jr.A	····			
00000120		1213		1E17	202E	2931		292D			)10.)-		
00000140		3A4A		3646	372C			464C			-@WAFL		
00000150			323E		5A50			4FFF			JQRO.		
00000160			OEOE		1113		1526				S805		
00000170		4F4F	4F4F	4F4F	4F4F	4F4F	4F 4F	4F4F			000000		
00000180		4F 4F	4F 4F	4F4F	4F4F	4F4F	4F4F	4F4F			000000		
00000190		4F4F	4F 4F	4F4F	4F4F	4F4F	4F4F	4F4F			000000		
000001A0		4F4F							0000.				
000001BC								C400					
00000100								0000					~
M IMAGE_00	0 🕅 IM	AGE 000										-	=
		//GE_000	<u> </u>										
Structure	Viewer (	(exif.hs	I)		<b>~</b>	+ ×	Compa	are Res	ults	All		-	\$
Address	Name	1			Value	- T			Sourc	e	Count		Т
€ 000000	)4 struc	t EXIF	HDR		{}								
		-			()								
			1				1				1		-
						2		1-	1 1	- 12		10.	2
]] \ Data Inspe	ctor AS	tructure	viewer	1		11	Compa	are ( Ch	hecksum A	Find A	Bookmarks	∖ Out	out /
Ready							Offset:	00000	004	Val	ue: -2048		1

# **Bug in the Fix**



# The fix contains a bug if the size is: 0xXX00

For example: 0x0100 becomes 0x01FF

#### **A Better Fix**

A better fix can be done without extending a section.

Changing only 2 bytes

### **A Better Fix**



05BF80 ADD 05BF84 MOV 05BF88 MOV 05BF8C MOV 05BF90 ADD 05BF94 STRB 05BF98 AND 05BF9C STRB

R1, R0, #0xFE ; OxFD R2, R1, LSL#16 R0, R2, LSR#16 R1, R0, LSR#8 R0, R3, #0xFE ; OxFD R1, [R4] R2, R1, #0xFF R0, [R4, #1]

#### **A Better Fix**



On the file patch:

#### Offset 0x4B380: 0xFE -> 0xFD Offset 0x4B390: 0xFE -> 0xFD



Exif header contains various fields: Date/time **Camera Vendor Camera Model** Artist Name aka your name in every image

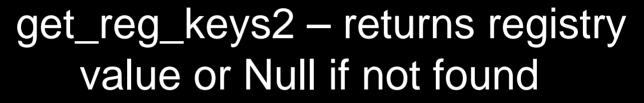


- Artist name comes from the Owner name stored on the phone.
- Camera.exe accesses name through the registry.
- From IDA string list:
   "ControlPanel\Owner\Owner"



#### Within the disassembly:

000481AC LDR R0, =aControlpanelOw 000481B0 MOV R3, #0x80000001 000481B4 MOV R2, #0x280 000481B8 MOV R1, R5 000481BC BL get\_reg\_key2 000481C0 CMP R0, #0 000481C4 BEQ done\_with\_regkeys



Change: 000481C0 00 00 50 E3 CMP R0, #0 To 000481C0 00 00 50 E1 CMP R0, R0; always equal

000481C4 BEQ done\_with\_regkeys



On the file patch:

#### Offset 0x0375C3: 0xE3 -> 0xE1





H	He	x Wo	orks	hop -	[IMAG	E 000	02.jp	gl									
10	File	e E	dit	Disk	Optio	ns To	ools	Window	Help	X						- 6	T X
Ī.	¥ =	a 🖪	8	1.%	h R	20	8 9	8 (B	1- 1	o B	e 1	QF	0 (	7 (-)		1 te	40010
]				00				• •=	1 101		S L	ųr	n Hr	2 E		14-	-
	≒ ^	• <<	>>	52	2 22 2	3 ~	<b>8</b> ∣	*/- +	- *	1 %	[<] [>]	A† a.	a A	₽ħ	昭 昭	2%	Щŀ
														144		-25	- 1
		000			FFE1	OOEC						· · · · <u>-</u>	.Exi	f]	I*.		^
		000		0800		0700	OFOI		0300	0000	4854				.HT		
		000		4300		0200			6200 1B01	0000	1A01 0100	C		D			
		000		0000		0000	2801		0100		0200		.1				
		000		0000	3201	0200	1400		7900	0000	6987	2		.v.			
		000		0400		0000			0000	0000	4170				.Ap		
	000	000	70	6163	6865	0048	0000	0001	0000	0048	0000	ache.	Н		н		
		000		0001		0032	3030		3036	3A31	3820		2006	5:06:	18		
		000		3036	3A32	313A	3437		0003	9002	0014	06:21	:47.				
		000		0000		0000	0000		0004		0030				0		
		000		3231	3009	9203	0001		0000	0000	0002	210					
		000		A004		0000	0080		0003	A004	0001				200		
		0000		363A		3A31	3820		3A32	313A	3437	6:06:	10 0	16:21	200		
		0000		FFEO	0010	4A46	4946		0100		0001		FIF.		. 47		
		001			FFEO		4A46			FFD8	FFDB		.JFX				
		001		0043	OOOD	090A	OBOA		OBOA		OEOD	.c					
	000	001	20	<b>OF13</b>	2015	1312	1213	3 271C	1E17	202E	2931				.)1		
	000	001	30	302E	292D	2033	3A4A	A 3E33	3646	372C	2D40	0.)-,	3:J>	36F7	,-@		
		001		5741	464C	4E52	5352		5A61	5A50	604A	WAFLN					
		001		5152	4FFF		430:		0E13	1113	2615	QRO					
		001		1526	4F35	2D35	4F4E		4F4F	4F4F	4F4F	.&05-					
		001		4F4F	4F4F	4F4F	4F4E		4F4F	4F4F	4F4F	00000					
		001		4F4F 4F4F	4F4F 4F4F	4F4F 4F4F	4F4F 4F4F		4F4F	4F4F	4F4F 7800	00000					
		001		4r 4r A003	0122		110		01FF	DDOO	0400	100000	000.	• • • •	•ו		
		001		OAFF		1F00		1 0501	0101	0101	0100		• • • •				
					0000			1 0203			0809						
4	_			-													
4	ST IM	AGE_	_000.														
×	Stru	uctur	e Vi	ewer	(exif.hs	l)			+ *	Compa	are Res	ults	All			•	\$
Ī	Ad	dres	s /	Name	ð.			Value				Sour	ce	(	Count		Т
	£00	0000	004	struc	t EXIF_	HDR		{}									
					-			. ,									
	I																
	<					i.			>	<							>
	1	ata In:	spect		tructure	Viewer			≤		are Ct	necksum	λ Find	λ Boo	kmarks	λ Out	22000
Re	adv					- new cl	/		111	Offset:					-5120	1 004	1
110	auy								_	Unset.	50000	001	1	alue.	5120		11

# Future of 3<sup>rd</sup> party patches

- Continued release of 3<sup>rd</sup> party security patches
- Advisories released with binary fix diffs
- Vulnerability market consisting of both 0day exploit and 0day patches

#### **Questions**?





#### **Shameless Self-Promotion**

Automating Exploit Detection: Cutting-edge Tools and Techniques Matt Hargett & Luis Miras Blackhat Training USA

Bridging the Gap between Static & Dynamic Reversing Defcon 14