Pwnium: element 1337

Chris Evans, Senior Troublemaker, Google

Surprise rewards time!

- "Last man standing award"
- "Specific achievement award"

Reward :: Last Man Standing

@miaubiz: $10,000

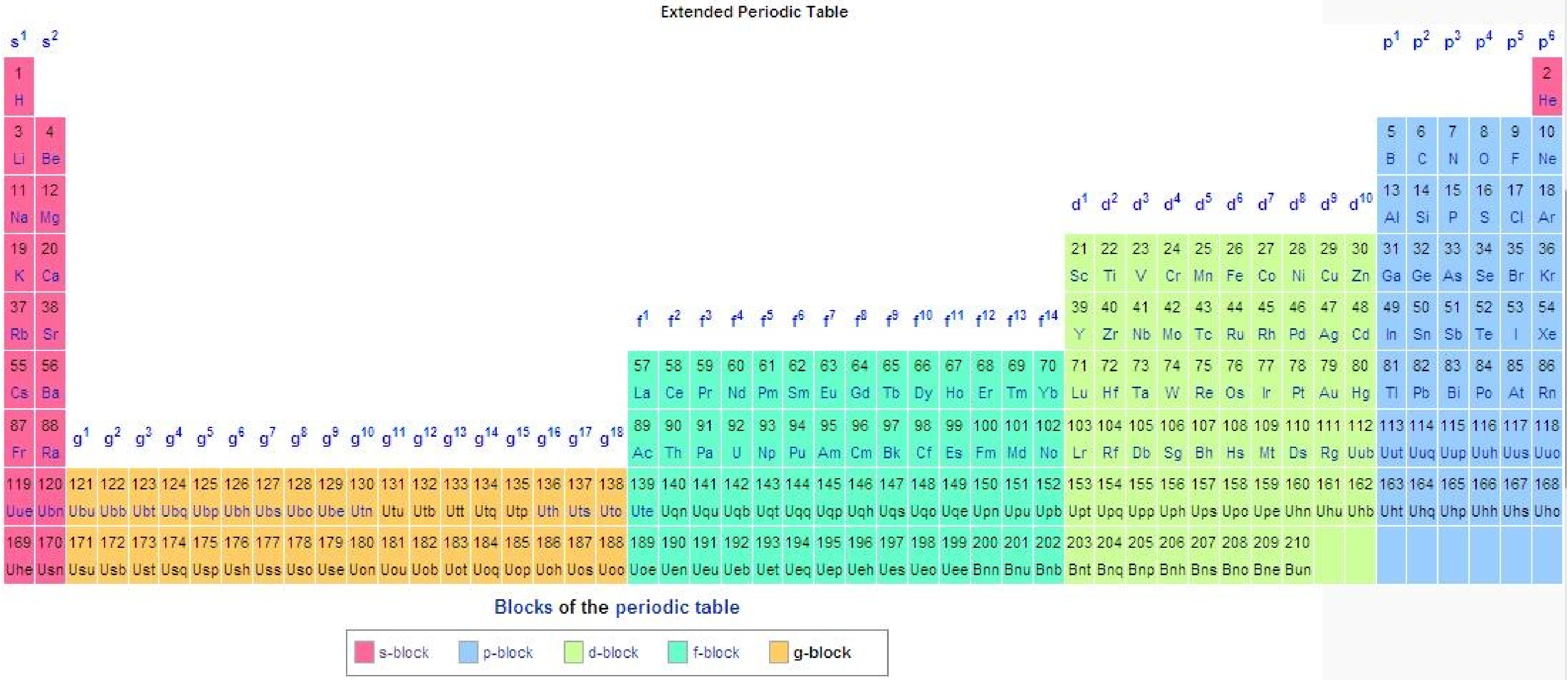
@miaubiz: @scarybeasts just gave u lots of cash on stage lol lol kittens

Reward :: Last Man Standing

@attekett: $10,000

Reward :: Specific Achievement (v8)

@mozdeco: $10,000



Extended Periodic Table

s^1	s^2																																											p^1	p^2	p^3	p^4	p^5	p^6
1 H																																																	2 He
3 Li	4 Be																																											5 B	6 C	7 N	8 O	9 F	10 Ne
11 Na	12 Mg																																	d^1	d^2	d^3	d^4	d^5	d^6	d^7	d^8	d^9	d^{10}	13 Al	14 Si	15 P	16 S	17 Cl	18 Ar
19 K	20 Ca																																	21 Sc	22 Ti	23 V	24 Cr	25 Mn	26 Fe	27 Co	28 Ni	29 Cu	30 Zn	31 Ga	32 Ge	33 As	34 Se	35 Br	36 Kr
37 Rb	38 Sr																			f^1	f^2	f^3	f^4	f^5	f^6	f^7	f^8	f^9	f^{10}	f^{11}	f^{12}	f^{13}	f^{14}	39 Y	40 Zr	41 Nb	42 Mo	43 Tc	44 Ru	45 Rh	46 Pd	47 Ag	48 Cd	49 In	50 Sn	51 Sb	52 Te	53 I	54 Xe
55 Cs	56 Ba																			57 La	58 Ce	59 Pr	60 Nd	61 Pm	62 Sm	63 Eu	64 Gd	65 Tb	66 Dy	67 Ho	68 Er	69 Tm	70 Yb	71 Lu	72 Hf	73 Ta	74 W	75 Re	76 Os	77 Ir	78 Pt	79 Au	80 Hg	81 Tl	82 Pb	83 Bi	84 Po	85 At	86 Rn
87 Fr	88 Ra	g^1	g^2	g^3	g^4	g^5	g^6	g^7	g^8	g^9	g^{10}	g^{11}	g^{12}	g^{13}	g^{14}	g^{15}	g^{16}	g^{17}	g^{18}	89 Ac	90 Th	91 Pa	92 U	93 Np	94 Pu	95 Am	96 Cm	97 Bk	98 Cf	99 Es	100 Fm	101 Md	102 No	103 Lr	104 Rf	105 Db	106 Sg	107 Bh	108 Hs	109 Mt	110 Ds	111 Rg	112 Uub	113 Uut	114 Uuq	115 Uup	116 Uuh	117 Uus	118 Uuo
119 Uue	120 Ubn	121 Ubu	122 Ubb	123 Ubt	124 Ubq	125 Ubp	126 Ubh	127 Ubs	128 Ubo	129 Ube	130 Utn	131 Utu	132 Utb	133 Utt	134 Utq	135 Utp	136 Uth	137 Uts	138 Uto	139 Ute	140 Uqn	141 Uqu	142 Uqb	143 Uqt	144 Uqq	145 Uqp	146 Uqh	147 Uqs	148 Uqo	149 Uqe	150 Upn	151 Upu	152 Upb	153 Upt	154 Upq	155 Upp	156 Uph	157 Ups	158 Upo	159 Upe	160 Uhn	161 Uhu	162 Uhb	163 Uht	164 Uhq	165 Uhp	166 Uhh	167 Uhs	168 Uho
169 Uhe	170 Usn	171 Usu	172 Usb	173 Ust	174 Usq	175 Usp	176 Ush	177 Uss	178 Uso	179 Use	180 Uon	181 Uou	182 Uob	183 Uot	184 Uoq	185 Uop	186 Uoh	187 Uos	188 Uoo	189 Uoe	190 Uen	191 Ueu	192 Ueb	193 Uet	194 Ueq	195 Uep	196 Ueh	197 Ues	198 Ueo	199 Uee	200 Bnn	201 Bnu	202 Bnb	203 Bnt	204 Bnq	205 Bnp	206 Bnh	207 Bns	208 Bno	209 Bne	210 Bun								

Blocks of the periodic table

🟥 s-block 🟦 p-block 🟩 d-block 🟩 f-block 🟨 g-block

1337

Pwn

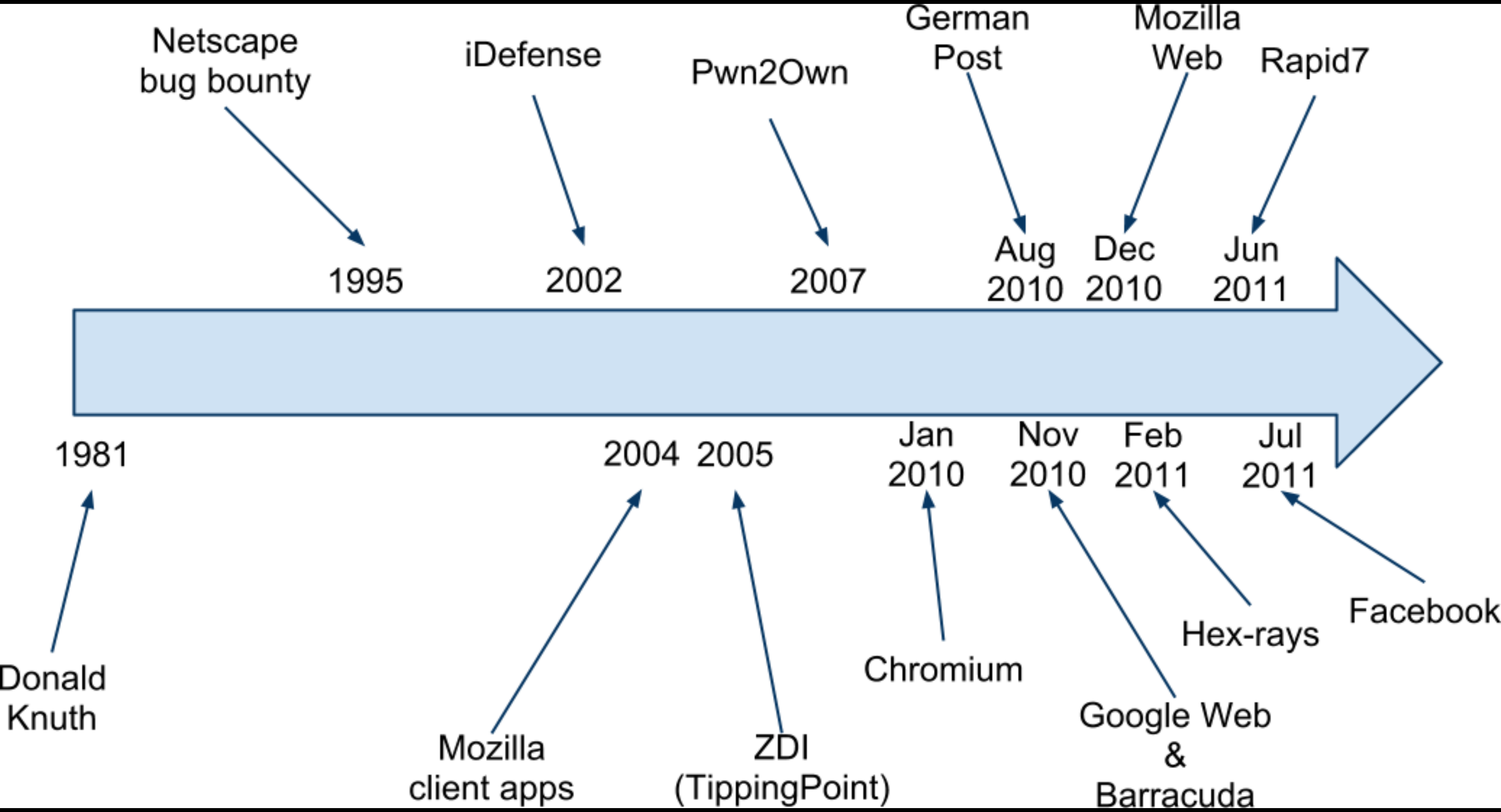
Pwnium

Agenda

1. Surprise rewards
2. History of reward programs
3. History of Pwnium
4. Tales from the war room
5. $$ and other stats

1337. Pwnium 2: results
1338. Q & A

History :: Timeline



Donald Knuth
1981

Netscape bug bounty
1995

iDefense
2002

Mozilla client apps
2004

ZDI (TippingPoint)
2005

Pwn2Own
2007

Chromium
Jan 2010

German Post
Aug 2010

Google Web & Barracuda
Nov 2010

Mozilla Web
Dec 2010

Hex-rays
Feb 2011

Rapid7
Jun 2011

Facebook
Jul 2011

History :: Recent Programs

Recently:

- Nov 2011: Secunia
- May 2012: Samsung (TV)
  - Empy Hall Of Fame :-(https://samsungtvbounty.com/content/white-hats
- June 2012: PayPal
  - "I originally had reservations about the idea of paying researchers for bug reports, but I am happy to admit that the data has shown me to be wrong"
- Sep 2012: Etsy

History :: Chromium VRP

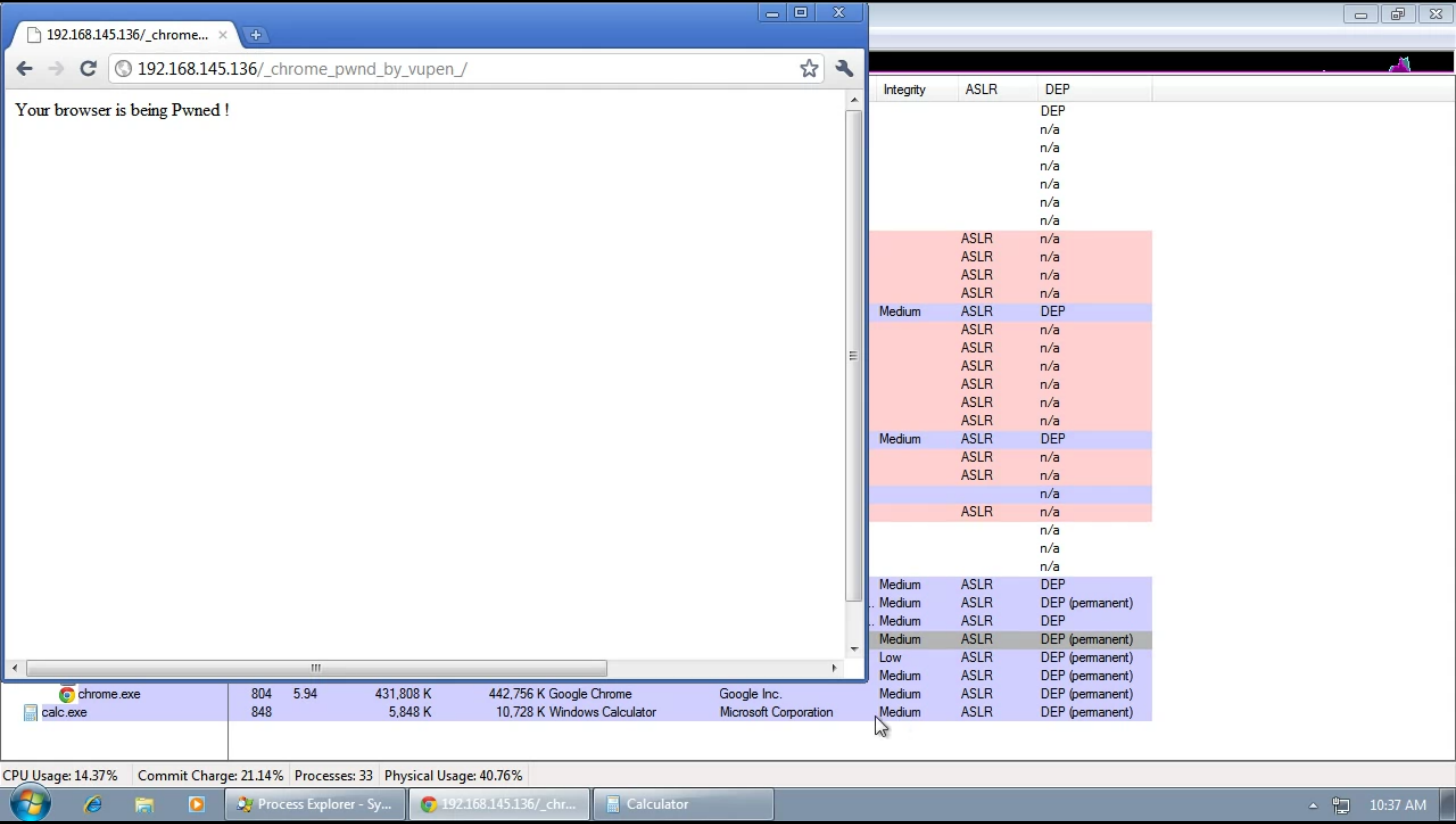
- Jan 2010: Launched, $500 - $1337
- July 2010: Top reward increased to $3133.7
- Feb 2012: Scope expanded to Chrome OS (Linux kernel, Flash, ...) plus bonuses for fixes
- Aug 2012: More bonuses, top reward of $10,000+
  - More flexibility to focus on exploitability

History :: Pwnium

- Feb 2011: Google sponsors $20,000 top-up reward for Chrome at Pwn2Own 2011
- Feb 2012: Agreed sponsorship of Pwn2Own 2012 with ZDI
- Feb 2012: ZDI misunderstands agreement
- Feb 2012: Pwnium announced
- Mar 2012: Pwnium surpasses wildest expectations
- Oct 2012: Pwnium 2

Tales from the war room

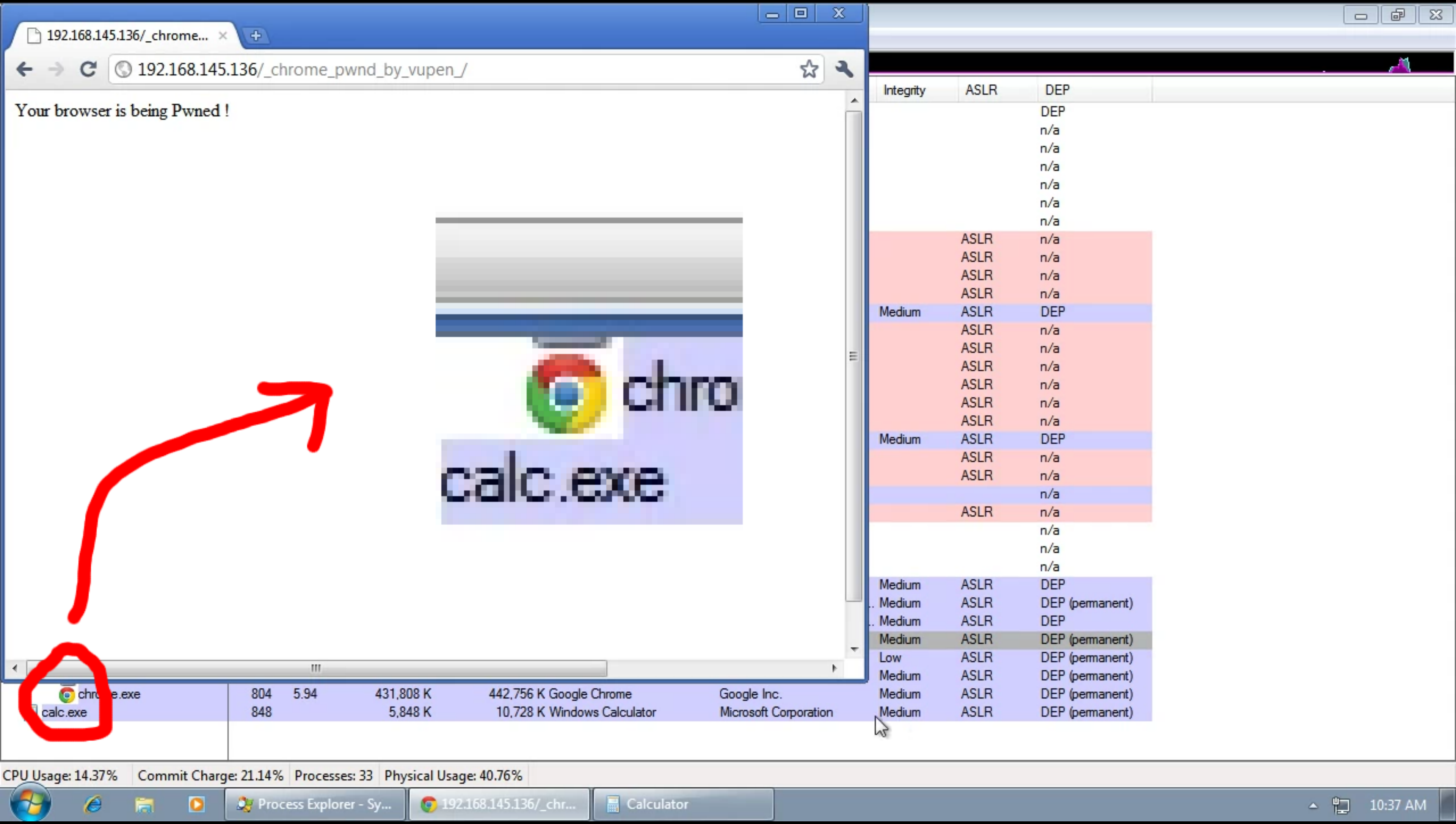
- May 2011: VUPEN non-disclosure
- Non-disclosed via ~~interpretive dance~~ YouTube video
- Normal security team?
  - Unverifiable claim => ignore
  - Hand off to PR team
- Google Security Team?


192.168.145.136/_chrome...
192.168.145.136/_chrome_pwnd_by_vupen_/

Your browser is being Pwned !

							Integrity	ASLR	DEP
									DEP
									n/a
									n/a
									n/a
									n/a
									n/a
									n/a
								ASLR	n/a
								ASLR	n/a
								ASLR	n/a
								ASLR	n/a
							Medium	ASLR	DEP
								ASLR	n/a
								ASLR	n/a
								ASLR	n/a
								ASLR	n/a
								ASLR	n/a
								ASLR	n/a
							Medium	ASLR	DEP
								ASLR	n/a
								ASLR	n/a
									n/a
								ASLR	n/a
									n/a
									n/a
									n/a
							Medium	ASLR	DEP
							Medium	ASLR	DEP (permanent)
							Medium	ASLR	DEP
							Medium	ASLR	DEP (permanent)
							Low	ASLR	DEP (permanent)
							Medium	ASLR	DEP (permanent)
chrome.exe	804	5.94	431,808 K	442,756 K	Google Chrome	Google Inc.	Medium	ASLR	DEP (permanent)
calc.exe	848		5,848 K	10,728 K	Windows Calculator	Microsoft Corporation	Medium	ASLR	DEP (permanent)

CPU Usage: 14.37% Commit Charge: 21.14% Processes: 33 Physical Usage: 40.76%



192.168.145.136/_chrome...

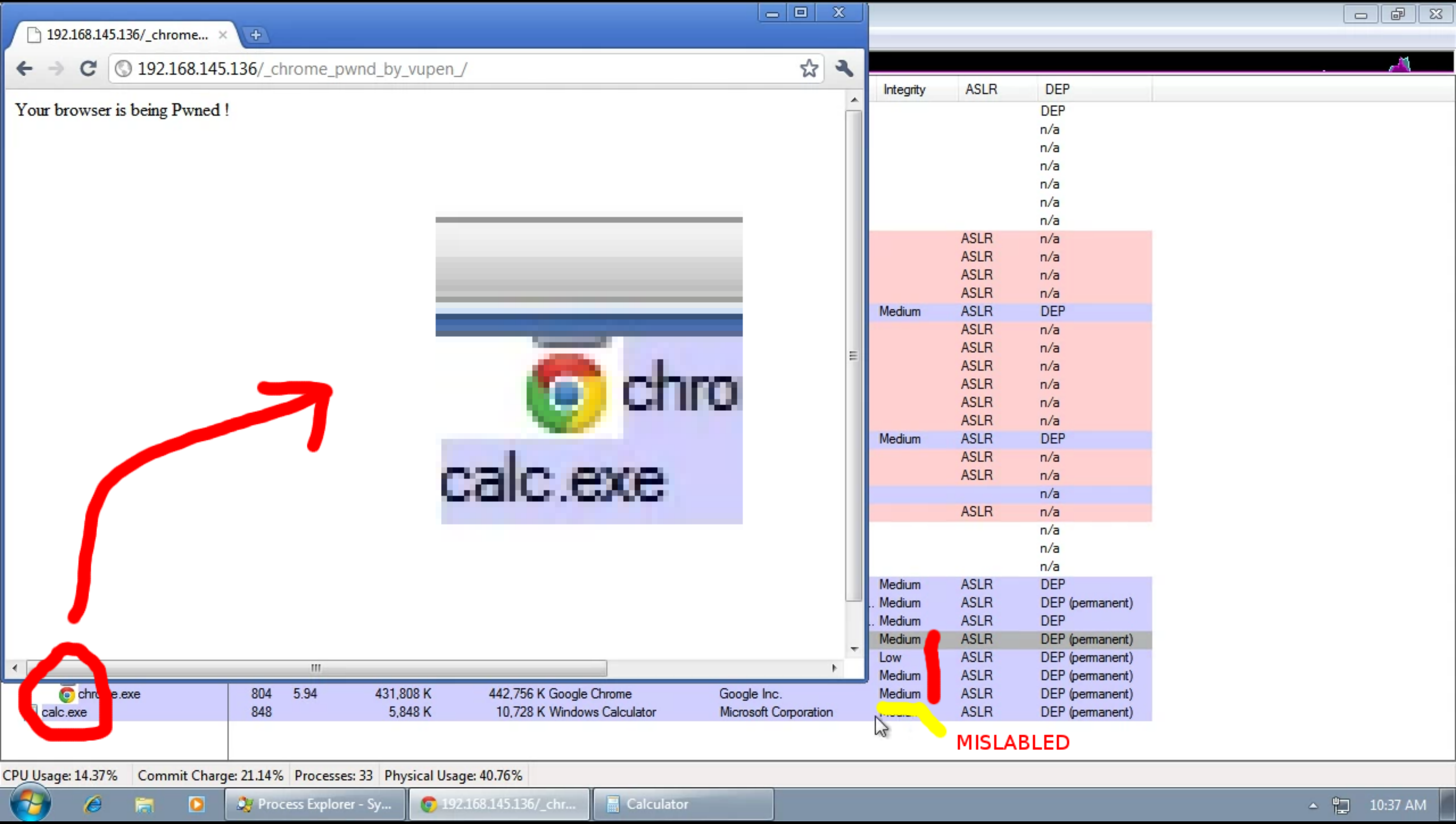
192.168.145.136/_chrome_pwnd_by_vupen_/

Your browser is being Pwned !

Integrity	ASLR	DEP
		DEP
		n/a
		n/a
		n/a
		n/a
		n/a
		n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
Medium	ASLR	DEP
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
Medium	ASLR	DEP
	ASLR	n/a
	ASLR	n/a
		n/a
	ASLR	n/a
		n/a
		n/a
		n/a
Medium	ASLR	DEP
Medium	ASLR	DEP (permanent)
Medium	ASLR	DEP
Medium	ASLR	DEP (permanent)
Low	ASLR	DEP (permanent)
Medium	ASLR	DEP (permanent)

```
chrome.exe  804  5.94  431,808 K  442,756 K Google Chrome       Google Inc.            Medium  ASLR  DEP (permanent)
calc.exe    848           5,848 K   10,728 K Windows Calculator  Microsoft Corporation  Medium  ASLR  DEP (permanent)
```

CPU Usage: 14.37% Commit Charge: 21.14% Processes: 33 Physical Usage: 40.76%



192.168.145.136/_chrome...

192.168.145.136/_chrome_pwnd_by_vupen_/

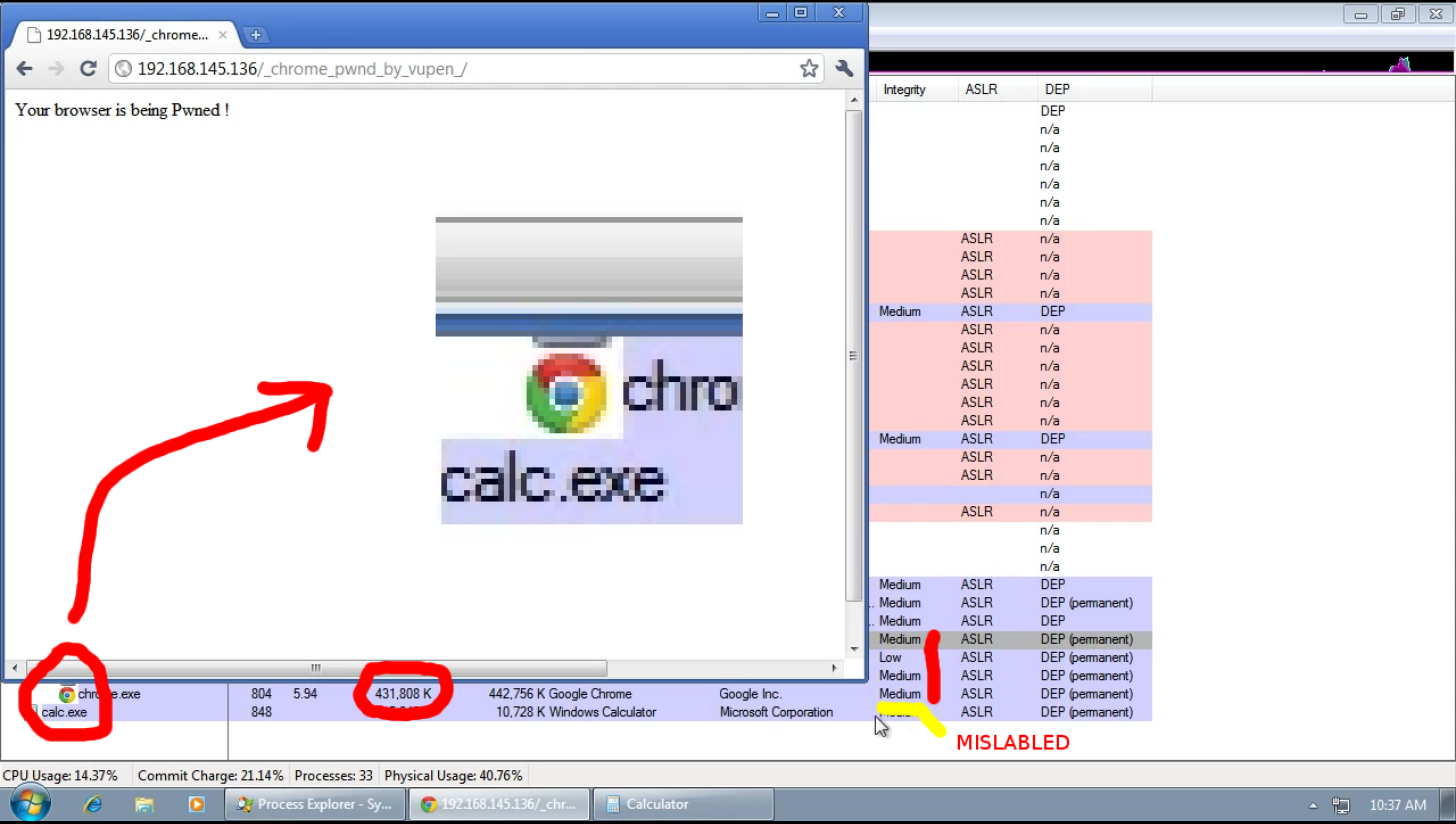
Your browser is being Pwned !

Integrity	ASLR	DEP
		DEP
		n/a
		n/a
		n/a
		n/a
		n/a
		n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
Medium	ASLR	DEP
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
Medium	ASLR	DEP
	ASLR	n/a
	ASLR	n/a
		n/a
	ASLR	n/a
		n/a
		n/a
		n/a
Medium	ASLR	DEP
Medium	ASLR	DEP (permanent)
Medium	ASLR	DEP
Medium	ASLR	DEP (permanent)
Low	ASLR	DEP (permanent)
Medium	ASLR	DEP (permanent)
Medium	ASLR	DEP (permanent)
	ASLR	DEP (permanent)

chrome.exe	804	5.94	431,808 K	442,756 K	Google Chrome	Google Inc.	Medium	ASLR	DEP (permanent)
calc.exe	848		5,848 K	10,728 K	Windows Calculator	Microsoft Corporation		ASLR	DEP (permanent)

MISLABLED

CPU Usage: 14.37% Commit Charge: 21.14% Processes: 33 Physical Usage: 40.76%



192.168.145.136/_chrome_pwnd_by_vupen_/

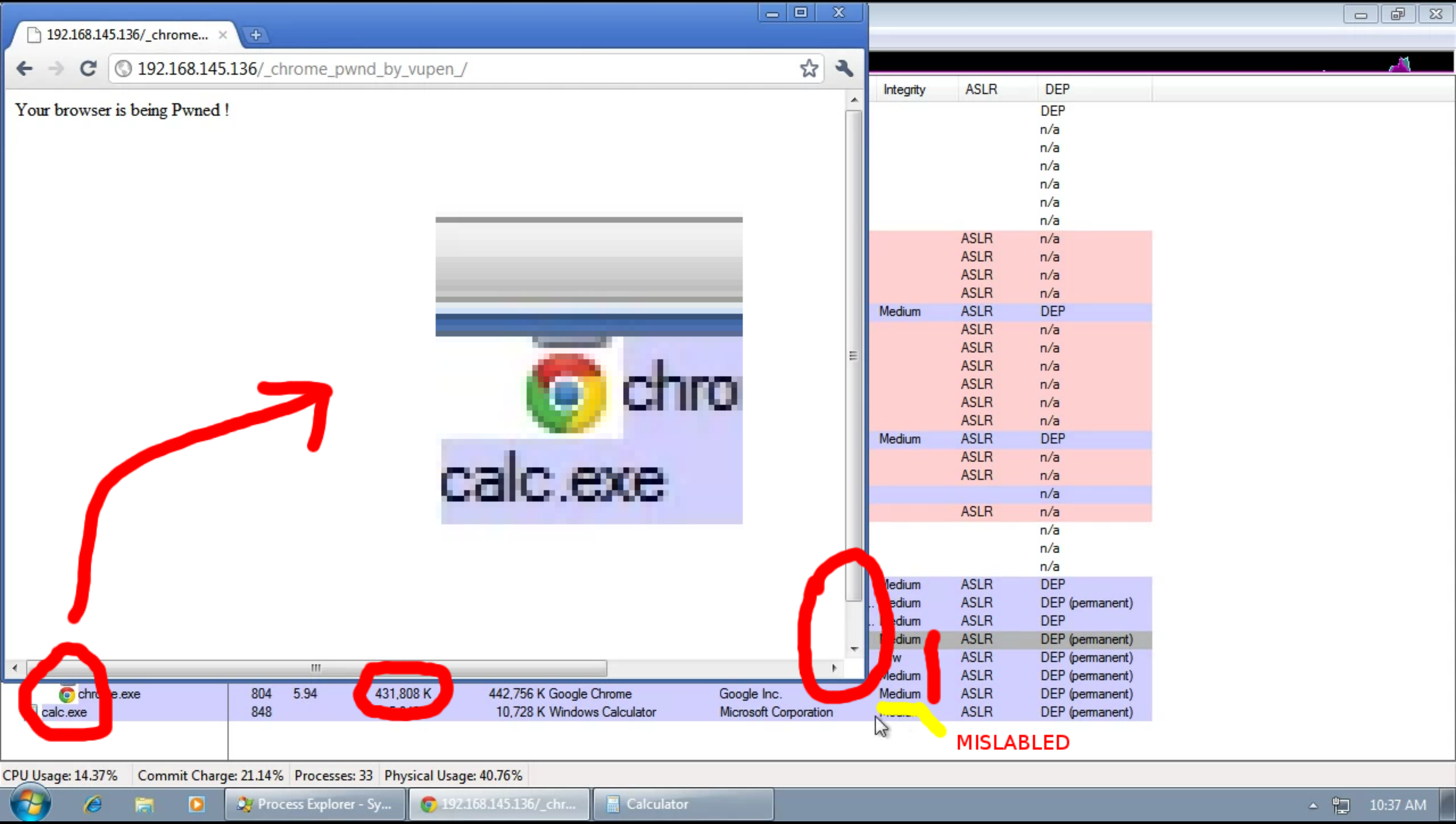
Your browser is being Pwned !

Integrity	ASLR	DEP
		DEP
		n/a
		n/a
		n/a
		n/a
		n/a
		n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
Medium	ASLR	DEP
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
Medium	ASLR	DEP
	ASLR	n/a
	ASLR	n/a
		n/a
	ASLR	n/a
		n/a
		n/a
		n/a
Medium	ASLR	DEP
Medium	ASLR	DEP (permanent)
Medium	ASLR	DEP
Medium	ASLR	DEP (permanent)
Low	ASLR	DEP (permanent)
Medium	ASLR	DEP (permanent)
Medium	ASLR	DEP (permanent)
Medium	ASLR	DEP (permanent)

chrome.exe	804	5.94	431,808 K	442,756 K	Google Chrome	Google Inc.
calc.exe	848			10,728 K	Windows Calculator	Microsoft Corporation

MISLABLED

CPU Usage: 14.37% Commit Charge: 21.14% Processes: 33 Physical Usage: 40.76%



192.168.145.136/_chrome...
192.168.145.136/_chrome_pwnd_by_vupen_/

Your browser is being Pwned !

Integrity	ASLR	DEP
		DEP
		n/a
		n/a
		n/a
		n/a
		n/a
		n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
Medium	ASLR	DEP
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
	ASLR	n/a
Medium	ASLR	DEP
	ASLR	n/a
	ASLR	n/a
		n/a
	ASLR	n/a
		n/a
		n/a
		n/a
ledium	ASLR	DEP
edium	ASLR	DEP (permanent)
edium	ASLR	DEP
dium	ASLR	DEP (permanent)
w	ASLR	DEP (permanent)
Medium	ASLR	DEP (permanent)
Medium	ASLR	DEP (permanent)
	ASLR	DEP (permanent)

chr e.exe	804	5.94	431,808 K	442,756 K	Google Chrome	Google Inc.
calc.exe	848			10,728 K	Windows Calculator	Microsoft Corporation

MISLABLED

CPU Usage: 14.37% | Commit Charge: 21.14% | Processes: 33 | Physical Usage: 40.76%

War room :: VUPEN :: response

- Flash security rampage
  - "Bring out the Tavis"
  - 20,000 files; 2,000 CPU cores; ~100 bugs
- Flash sandbox rampage
  - Add missing UIPI protections
  - Found Flash broker memory corruptions
  - Accelerate work on Pepper Flash
- Flash JIT spray protection rampage
  - 0xabad1dea
- Invite community to rampage
  - Flash vulnerabilities now included in Chromium Rewards Program!

$$ and other stats

- Total rewards issued: 485
- Total reward payout?

$$ and other stats

- Total rewards issued: 485
- Total reward payout?

2,001,350

$$ and other stats

- Total rewards issued: 485
- Total reward payout?

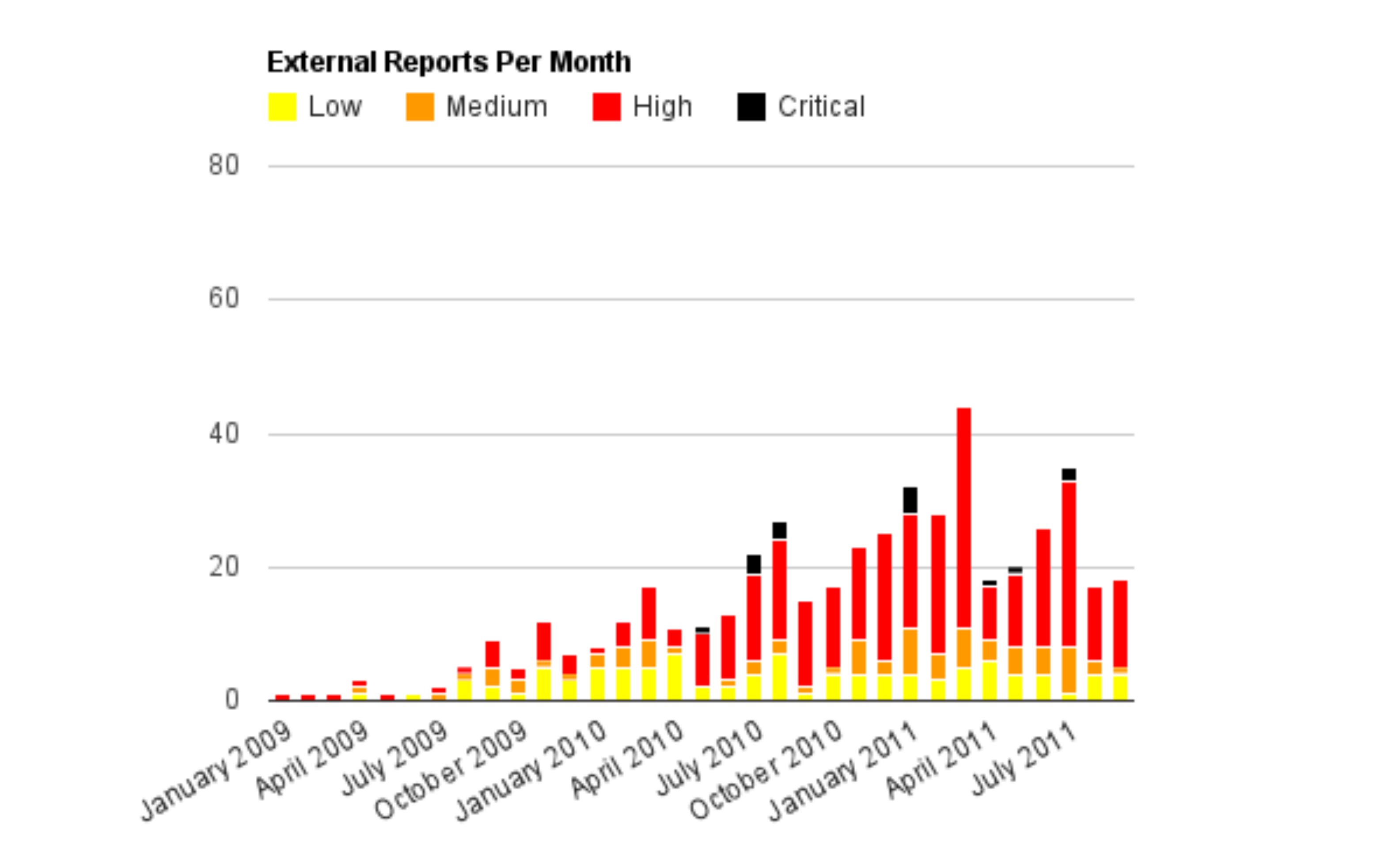
2,001,350

$$ and other stats

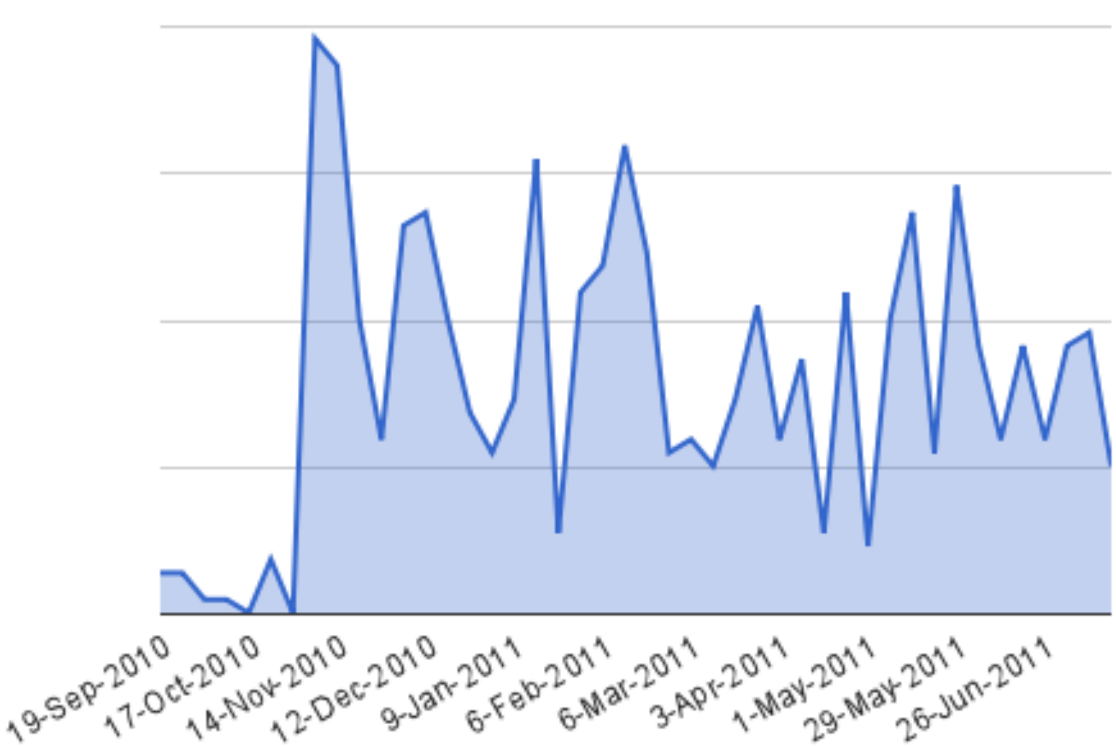
- Total rewards issued: 485
- Total reward payout?

$650,000 (>> $1M including web program)

Stats :: VRP launch 1 :: Chromium



Stats :: VRP launch 2 :: Web



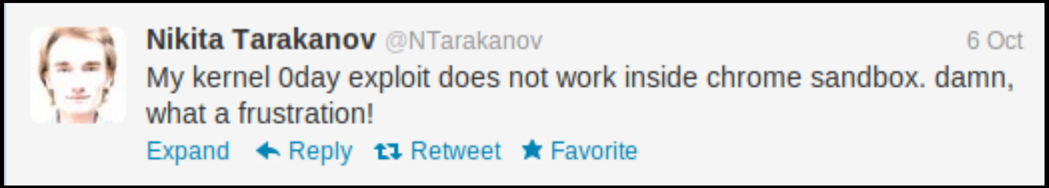
Pwnium 2 :: results

- @NTarakanov non-entry
  - Dispels "no-one entered!" myth
- Pinkie Pie entry

Pwnium 2 :: @NTarakanov

- Kernel (driver) vulnerability
  - Broadcom wireless driver specific to Pwnium laptop
  - Buggy ioctl implementation
- Leading to.....

Pwnium 2 :: @NTarakanov



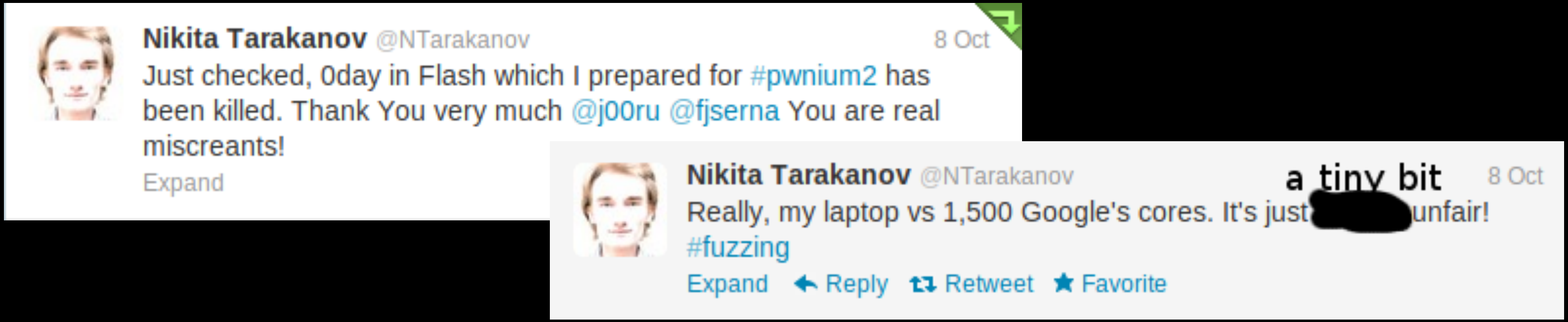
Nikita Tarakanov @NTarakanov 6 Oct

My kernel 0day exploit does not work inside chrome sandbox. damn, what a frustration!

ONE DOES NOT SIMPLY
EXPECT DEVICE HANDLES TO WORK INSIDE THE CHROME SANDBOX

Pwnium 2 :: @NTarakanov

- Shame to waste a powerful bug!
  - 0day dropped thanks to Pwnium 2!
  - http://pastebin.com/P1nACjxR
- But how to get code execution inside sandbox in the first place?

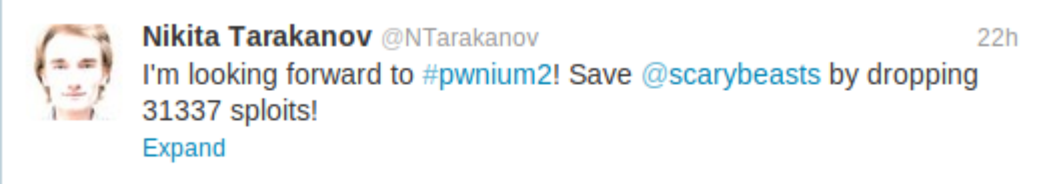


Nikita Tarakanov @NTarakanov 8 Oct

Just checked, 0day in Flash which I prepared for #pwnium2 has been killed. Thank You very much @j00ru @fjserna You are real miscreants!

Nikita Tarakanov @NTarakanov a tiny bit 8 Oct

Really, my laptop vs 1,500 Google's cores. It's just [redacted] unfair! #fuzzing



Nikita Tarakanov @NTarakanov 22h

I'm looking forward to #pwnium2! Save @scarybeasts by dropping 31337 sploits!

Pwnium 2 :: Pinkie Pie

- Confirmed $60,000 win!!

Pwnium 2 :: Pinkie Pie :: Patch

- OMG
  - Same-day patch (Malaysian time)
  - Patched overnight (California time)
  - ~12hr turnaround
  - Beat our own record
- LOL
  - This wasn't a real emergency
    - Not an 0day
      - Try and use the term correctly
        - Arbitrary and excessive indentation
  - Nice to give the engines a test fire though!

PROPERTY
OF A&F
'54
CELEBRATING A DECADE OF HITB
Vector
ystems
[redacted]

OMG!! PLEASE don't be in FLASH
PROPERTY OF A&F '54
Vector Systems

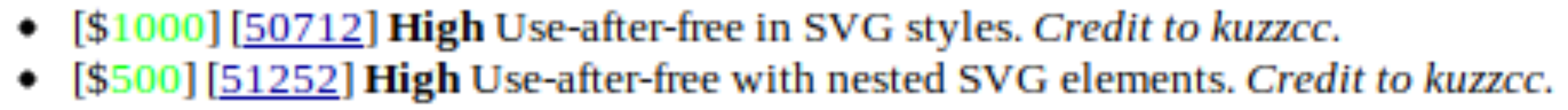
$$$
PROPERTY
OF PINKIE PIE
'54
Vector
Systems
OMG!! PLEASE don't be in FLASH

Pwnium
Google
COR-O-VAN

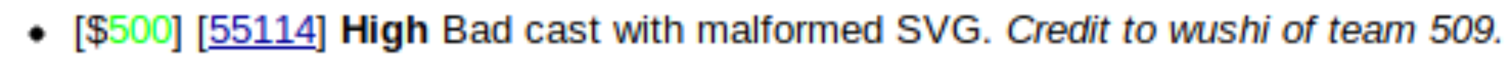
Pwnium #2 Away Team
- scarybeasts
Owned by Pinkie Pie

Pwnium 2 :: Pinkie Pie :: Details

- Phase 1a: Find bug inside renderer sandbox
  - SVG bug
  - Use after free!
    - (Let's be honest, what did you expect?)
    - SVG already has a <use> tag, we might as well have a <free> tag :-/
- Meanwhile, in Sep 2010.....



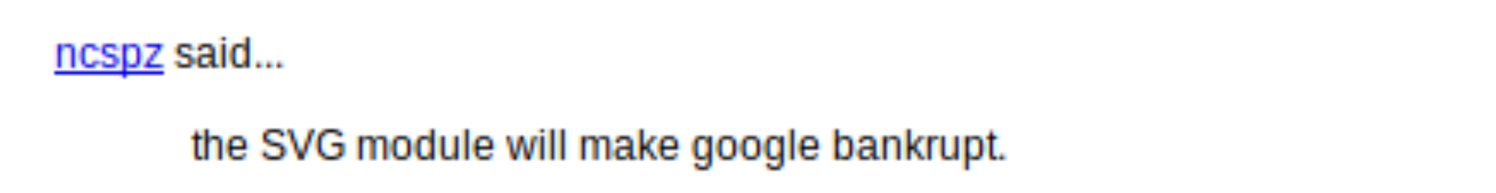
- [$1000] [50712] **High** Use-after-free in SVG styles. *Credit to kuzzcc.*
- [$500] [51252] **High** Use-after-free with nested SVG elements. *Credit to kuzzcc.*



- [$500] [55114] **High** Bad cast with malformed SVG. *Credit to wushi of team 509.*

And there was a visionary known only as "ncspz".....

Pwnium 2 :: Pinkie Pie :: SVG

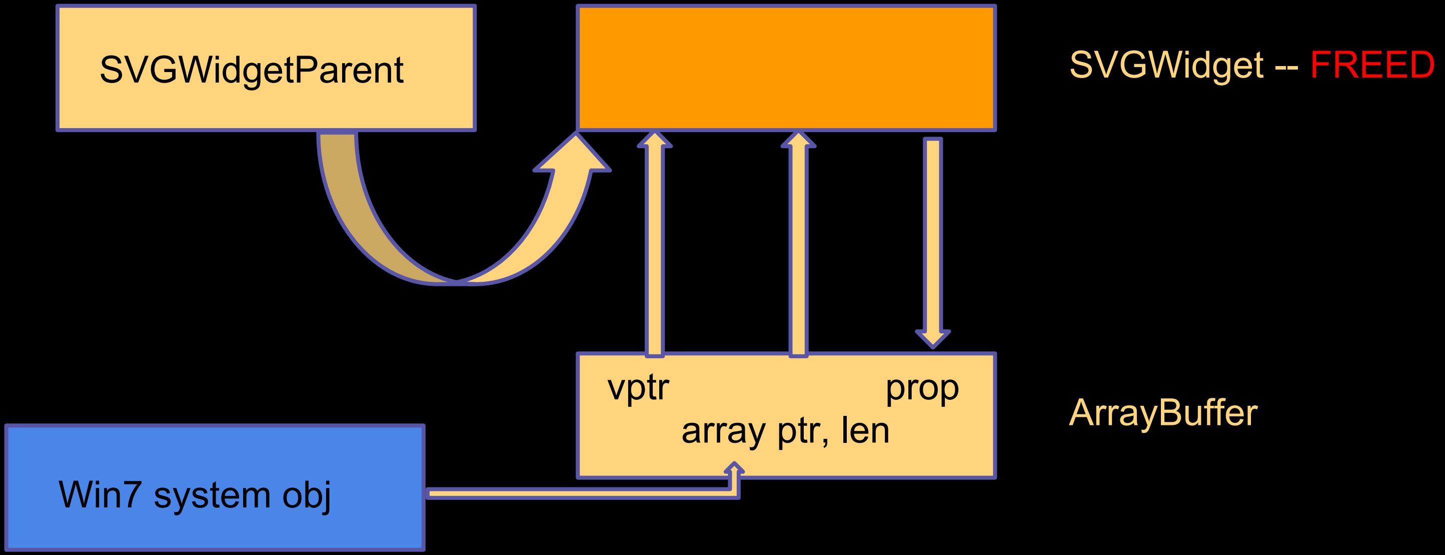


ncspz said...

the SVG module will make google bankrupt.

Pwnium 2 :: Pinkie Pie :: Details

- Phase 1b: convert use-after-free into code execution inside sandbox!
  - Force garbage collection
  - Allocate "ArrayBuffer" objects of same size as freed object

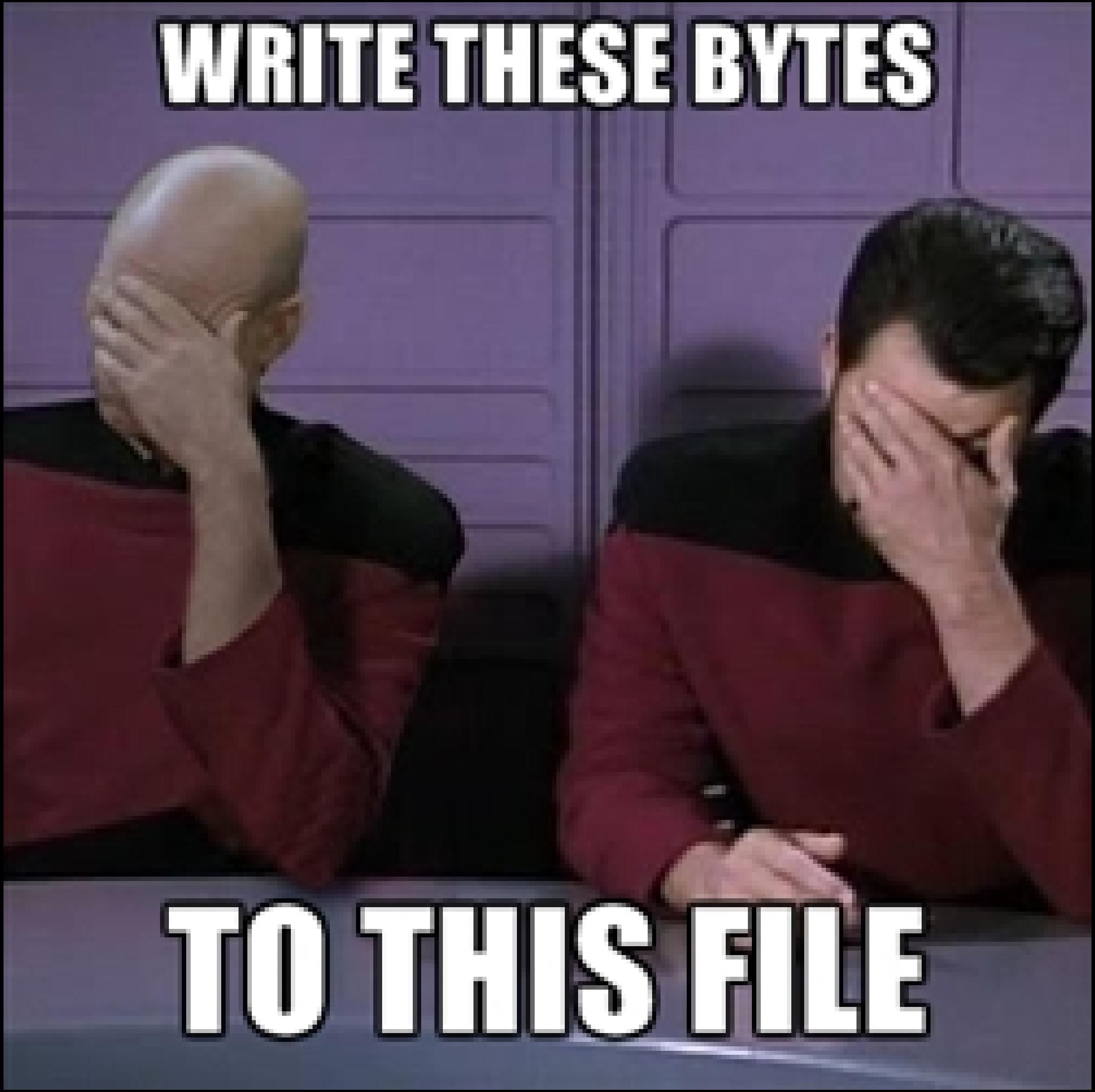


Pwnium 2 :: Pinkie Pie :: Details

- Phase 1b (continued)
  - Populate ArrayBuffer with a pointer to a Win7 system object at right offset
    - Actually used as a pointer to an array that can be read via JS
    - Win7 system object at predictable location :(
      - You don't really have have ASLR
      - Worst kept well-known secret?
      - Allegedly fixed in Win8 64-bit
  - Follow pointers to locate heap, executable
  - Now have info needed to set up ROP
  - Populate beginning of ArrayBuffer with custom vtable pointer!
  - Kick off ROP

Pwnium 2 :: Pinkie Pie :: Details

- Phase 2: escape sandbox
  - Attack IPC messages
  - Semantics not syntactics
  - What fiendish complexity did Pinkie Pie unleash......?


WRITE THESE BYTES
TO THIS FILE

I DON'T ALWAYS WRITE FILES BASED ON UNTRUSTED IPC MESSAGES
BUT WHEN I DO, I TRUST THE FILE, PATH AND CONTENT!

Q & A