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 lol kittens
Reward :: Last Man Standing

@attekett: $10,000
Reward :: Specific Achievement (v8)

@mozdeco: $10,000
Extended Periodic Table

Blocks of the periodic table

- s-block
- p-block
- d-block
- f-block
- g-block

1337
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
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?
Your browser is being Pwned!
Your browser is being Pwned!

[Image of Chrome and Calculator executables with highlighted elements]
Your browser is being Pwned!
Your browser is being Pwned!
Your browser is being Pwned!

![Chrome Logo](chrome.png)

`calc.exe`

![Process Explorer](process_explorer.png)

**MISLABELED**
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!
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

External Reports Per Month

- Low
- Medium
- High
- Critical

January 2009 to July 2011
Stats :: VRP launch 2 :: Web
Pwnium 2 :: results

- @NTarakanov non-entry
  - Dispels "no-one entered!" myth
- Pinkie Pie entry
Kernel (driver) vulnerability
  ○ Broadcom wireless driver specific to Pwnium laptop
  ○ Buggy ioctl implementation

Leading to.....
Nikita Tarakanov @NTarakanov
My kernel Oday exploit does not work inside chrome sandbox. damn, what a frustration!
Expect device handles to work inside the Chrome sandbox.
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?
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!
Premier #2 Away Team

C.1.2ram - scarybeasts
Gamer - cdg
Agent - juggling
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".....
ncspz said...

the SVG module will make google bankrupt.
Phase 1b: convert use-after-free into code execution inside sandbox!
- Force garbage collection
- Allocate "ArrayBuffer" objects of same size as freed object
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
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