Browser Exploitation (Firefox Rant)

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

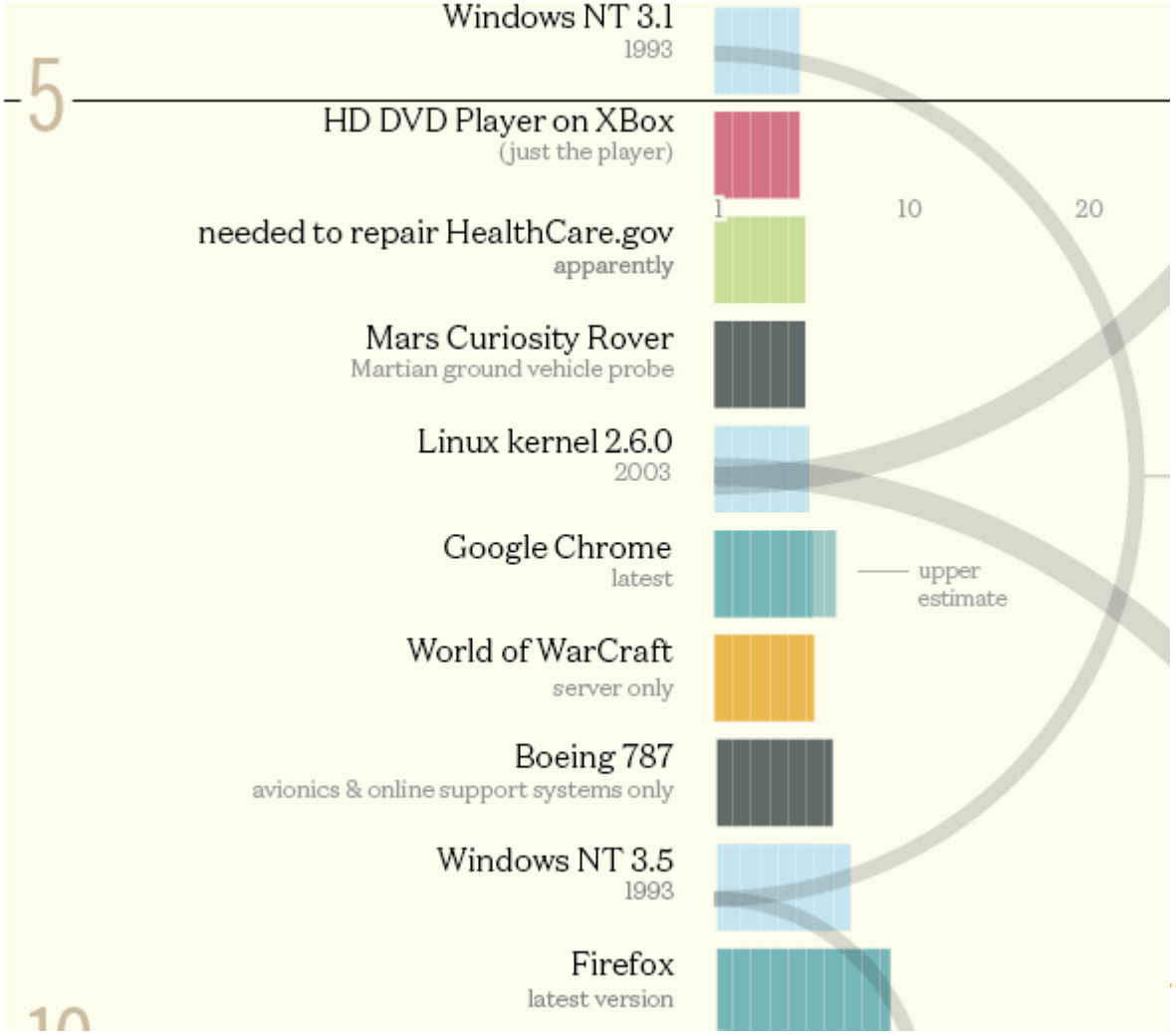
Browser security

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Browser security

Browser code size



Browser Security

Browsers:

Similar size like an OS

Support a shitload of file formats (PDF, GIF/PNG/JPEG, SVG, ...)

Can “upload” your own code (Javascript) to be executed!

Firefox Rant

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Firefox Rant

Rant: Firefox (2016)

Good:

- Full ASLR
- (Except on OSX for 3 years… and nobody noticed)

Bad:

- No Sandbox (yet)
- No 64 bit (yet)
- No process-per-tab (yet)
- No (professional) source code auditing / SDL
- No (professional) fuzzing
- Lots of untrusted, unaudited 3rd party addons, extensions etc.

Firefox Rant

Rant: Firefox (2017)

Good:

- Full ASLR
- (Except on OSX for 3 years… and nobody noticed)

Bad:

- No Sandbox (yet) -> “will be released soon” (since 3 years)
- No 64 bit (yet) -> 64 bit exists, but default is 32 bit
- No process-per-tab (yet) -> “will be released soon”
- No (professional) source code auditing / SDL
- No (professional) fuzzing -> More fuzzing is being done.
- Lots of untrusted, unaudited 3rd party addons, extensions etc.

But: The Firefox rendering engine (Gecko) will be replaced by Servo, written in Rust!

Firefox Rant

The history of “secure browsers”

- Some “secure browsers” completely disabled Same-origin-policy, ASLR, DEP etc.
- Making them the most insecure browsers EVER

My professional opinion:

- Most secure: Chrome, Edge
- Close: IE11

- Don’t use: Firefox (sorry), or any other browsers (Safari, IE8/9)
- Really don’t use: Torbrowser
  - Based on Firefox ESR (Long term support)
  - Every Torbrowser version therefore contains dozens, if not hundreds of publicly known exploits
  - Monocolture…

Firefox Rant

2014: George Hotz (geohot, wrote first PlayStation 3 and iOS/iPhone Exploits) wrote the first Chromebook Exploit for pwnium. And:

"Before pwnium, I had a few days extra, so I figured, why not try Firefox. Firefox, at least ca 2013, was about on par with a hard CTF problem. It took my 24 hours. 24 hours, full 0-day in Firefox.
A lot of people use this browser. Don't use it. Use Chrome."

USENIX Enigma 2016 - Timeless Debugging

- https://youtu.be/eGl6kpSajag?t=178

Firefox Rant

Even the FBI has Firefox Exploits…

As Ars has reported before, to breach the security normally afforded by Tor, the FBI deployed a "network investigative technique" (NIT). In a related case prosecuted out of New York, an FBI search warrant affidavit described both the pornography available to Playpen's 150,000 members and the NIT's capabilities. As a way to ensnare users, the FBI took control of Playpen and ran it for 13 days in 2015 before shutting it down. During that period, with many users' Tor-enabled digital shields down—revealing their true IP addresses—the government was able to identify and arrest the 135 child porn suspects.

Joshua Yabut, another researcher who also analyzed the code, told Ars it exploits a so-called use-after-free bug that requires JavaScript to be enabled on the vulnerable computer. Yabut went on to say the code is "100% effective for remote code execution on Windows systems." The exploit code, the researcher added, adjusts the memory location of the payload based on the version of Firefox being exploited. The versions span from 41 to 50, with version 45 ESR being the version used by the latest version of the Tor browser. The adjustments are an indication that the people who developed the attack tested it extensively to ensure it worked on multiple releases of Firefox. The exploit makes direct calls to kernel32.dll, a core part of the Windows operating system.

Firefox Rant

Web-browser / Mitigation	MS Internet Explorer 11	Microsoft Edge	Google Chrome	Mozilla Firefox
Sandbox	AppContainer (EPM)	AppContainer	AppContainer	
DEP	X	X	X	X
HEASLR, force relocate	XX	XX	X	ASLR
Dynamic code prohibited		X		
Strict handle checks	X	X	X	
Win32k system calls disabled			X	
Extension points disabled				
Control Flow Guard enabled	X	X		
Signatures restricted		X		
Non-system fonts disabled				
Loading of remote and low IL images disabled		X	X	

Table 9. Comparison of mitigations in web browsers.

References

Look Mom, I don’t use Shellcode

- Browser Exploitation Case Study for IE11
- Moritz Jodeit
- EKO12 (Ekoparty Security Conference)
- https://www.youtube.com/watch?v=PbIpd89efX8&index=14&list=PLdgOScViw-omMZQymL2SWKh5BLfMhDijB