

Questions, Issues,
Concerns, Suggestions
Welcome at any time
Even Now

Sun City Computer Club

Windows SIG

January 23, 2018

- Safer not Safe
- E-postcard not e-mail
- ADMINISTRATOR
- Passphrases not passwords
- Radio not wireless

Vocabulary



- Spectre and Meltdown
- speculative execution, branch prediction
- IoT
- Any/everything
- Kernel level code impacts
- Conspiracy??

Current Topics



- ALL (USA?) CPUs for last decade
- BIOS, Firmware, microcode
- Work on remediation ongoing for months
- Linux kernel
- Speculative execution pipelining
- Cache lines filled at exception
- Code on your system
- “Gathered” memory may be of value
- Remediation may affect performance
- Internet of Things Thing Things
- WEB and Virtual machines
- Games

Meltdown and Spectre

```
C:\Users\john\bin>SpecuCheck-x86.exe
SpecuCheck v1.0.5 -- Copyright(c) 2018 Alex Ionescu
https://ionescu007.github.io/SpecuCheck/ -- @aionescu
-----

Mitigations for CVE-2017-5754 [rogue data cache load]
-----
[-] Kernel VA Shadowing Enabled: yes
  └─> with User Pages Marked Global: no
  └─> with PCID Flushing Optimization (INVPCID): yes

Mitigations for CVE-2017-5715 [branch target injection]
-----
[-] Branch Prediction Mitigations Enabled: no
  └─> Disabled due to System Policy (Registry): no
  └─> Disabled due to Lack of Microcode Update: yes
[-] CPU Microcode Supports SPEC_CTRL MSR (048h): no
  └─> Windows will use IBRS (01h): no
  └─> Windows will use STIPB (02h): no
[-] CPU Microcode Supports PRED_CMD MSR (049h): no
  └─> Windows will use IBPB (01h): no
```

Advanced

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompat

- > PropertySystem
- > Proximity
- > PushNotifications
- QualityCompat
- > Reliability

Name	Type	Data
(Default)	REG_SZ	(value not set)
cadca5fe-87d3-4b96-b7fb-a231484277cc	REG_DWORD	0x00000000 (0)

Advanced



InSpectre: Check Spectre and Meltdown Prevention



InSpectre

Release #1

Check Windows operating system
and processor hardware safety.
Freeware by Steve Gibson / @Sggrc



Spectre & Meltdown Vulnerability and Performance Status

Vulnerable to Meltdown: **YES!**

Vulnerable to Spectre: **YES!**

Performance: **GOOD**

(full details below)

In early 2018 the PC industry was rocked by the revelation that

See GRC's InSpectre webpage at: <https://grc.com/inspectre.htm>
for a full explanation of the use and operation of this freeware utility.

Enable Meltdown Protection

Enable Spectre Protection

Exit



InSpectre

Release #1

Check Windows operating system and processor hardware safety.
Freeware by Steve Gibson / @Sggrc



update the system's hardware and software for maximum security and performance.

This system's present situation:

- This 64-bit version of Windows is **not aware of either the Spectre or Meltdown** problems. Since Intel processors are vulnerable to both of these attacks, this system will be vulnerable to these attacks until its operating system has been updated to handle and prevent these attacks.

See GRC's InSpectre webpage at: <https://grc.com/inspectre.htm> for a full explanation of the use and operation of this freeware utility.

Enable Meltdown Protection

Enable Spectre Protection

Exit

Task Manager

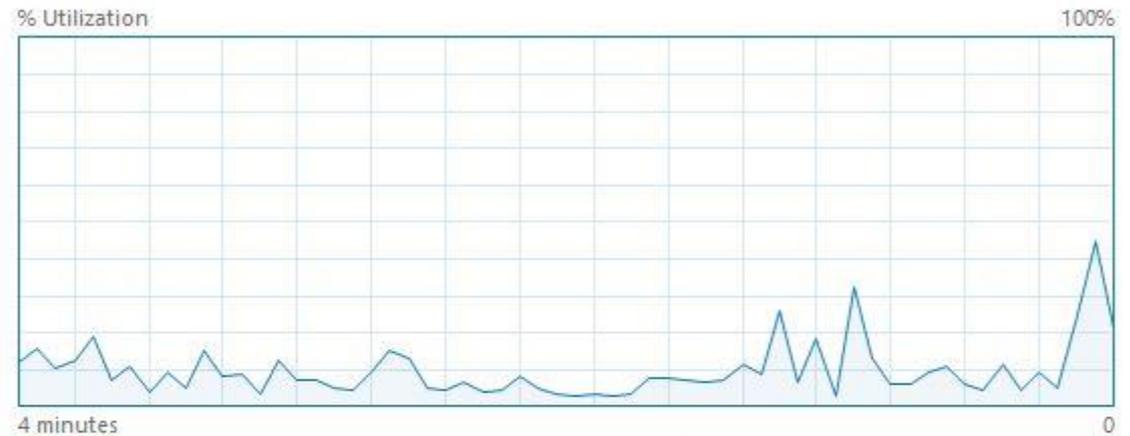
File Options View

Processes Performance App history Startup Users Details Services

- CPU**
21% 2.49 GHz
- Memory**
6.4/11.9 GB (54%)
- Disk 0 (C: D:)**
4%
- Ethernet**
S: 160 R: 88.0 Kbps
- Wi-Fi**
Not connected
- Bluetooth**
Not connected
- GPU 0**
Intel(R) HD Graphics 4600
2%

CPU

Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz



Utilization	Speed	Base speed:	3.20 GHz
21%	2.49 GHz	Sockets:	1
Processes	Threads	Cores:	4
232	3358	Logical processors:	4
Handles	Up time	Virtualization:	Disabled
108966	0:03:31:53	Hyper-V support:	Yes
		L1 cache:	256 KB
		L2 cache:	1.0 MB
		L3 cache:	6.0 MB

[Fewer details](#) | [Open Resource Monitor](#)

- Microsoft patch office docs ALL versions
- Office macros
- AOL and Verizon emails from Gmail domain
- Facebook Help “Foreign interference”

Current Topics

Find Friends



← Back

foreign interference



What is our action plan against foreign interference?

We've taken down fake accounts and Pages created by foreign actors attempting to interfere in the 2016 US Elections. [Check to see if you liked or followed a Facebook Page or Instagram account created by the Internet Research Agency - the organization associated with these accounts and Pages.](#)

- Patch Windows
backup, MCT, restore point
Check the patches
- Patch any/everything
backup, save settings & configurations
- Monitor news, accounts, environment
- Use multiple browser instances
- For sensitive sites
Use more secure browser
Use browser add-ons & extensions
Check those browser settings, add-ons, etc.

Suggestions

- BEFORE EACH sensitive session
 - Check add-ons and extensions for updates
 - Check browser for updates
 - Open ONE tab only
 - Use multi-factor authentication
 - Enable minimal settings
 - Check for online alerts
 - Monitor accounts
 - Close & exit browser

Client side ONLY

Suggestions

- Use Linux VM requires some effort
- Chromebook not to my liking
- Quad 9 DNS settings on devices
- Internet of Things
- Home infrastructure
- Use for old smart devices

Suggestions

The Adthink script contains very detailed categories for personal, financial, physical traits, as well as intents, interests and demographics. It is hard to comment on the exact use of these categories but it gives a glimpse of what our online profiles are made up of:

birth date, age, gender, nationality, height, weight, BMI (body mass index), hair_color (black, brown, blond, auburn, chestnut, red, gray, white), eye_color (amber, blue, brown, grey, green), education, occupation, net_income, raw_income, relationship states, seek_for_gender (m, f, transman, transwoman, couple), pets, location (postcode, town, state, country), loan (type, amount, duration, overindebted), insurance (car, motorbike, home, pet, health, life), card_risk (chargeback, fraud_attempt), has_car(make, model, type, registration, model year, fuel type), tobacco, alcohol, travel (from, to, departure, return), car_hire_driver_age, hotel_stars

[Audienceinsights.net](https://audienceinsights.net)

The image shows a web browser window with the URL `https://bonobos.com/account/wallet`. The page title is "Your Wallet | Bonobos". The main content is a "Wallet" form with the following fields:

- Add New Card** (Cancel button)
- NAME** (As it appears on your card): John Doe
- CARD NUMBER**: 4111111111111111 VISA
- MONTH**: 10, **YEAR**: 2020, **CVV**: 456
- Set Card as Default
- COUNTRY**: United States
- FIRST NAME**: John, **LAST NAME**: Doe
- ADDRESS**: 100 Main Street
- Chat with us button

The browser's developer tools are open to the Network tab, showing a list of requests. The following requests have their response bodies highlighted with red boxes:

- Request 4: `{When: 385423, Kind: 18, Args: [1047, "John Doe"]}`
- Request 6: `{Kind: 4, When: 385442, Args: [1872, "value", "2017-11-14"]}`
- Request 9: `{When: 385567, Kind: 15, Args: [1047, "John Doe"]}`
- Request 21: `{When: 386495, Kind: 13, Args: [72, 313]}`
- Request 23: `{When: 387544, Kind: 14, Args: [527, "4"]}`
- Request 25: `{When: 387638, Kind: 18, Args: [527, "41"]}`
- Request 27: `{When: 388887, Kind: 14, Args: [457, "41"]}`
- Request 29: `{When: 388166, Kind: 18, Args: [1047, "41"]}`
- Request 30: `{When: 388167, Kind: 15, Args: [457, "41"]}`
- Request 31: `{When: 388328, Kind: 14, Args: [457, "41"]}`
- Request 32: `{When: 388422, Kind: 18, Args: [1047, "41"]}`
- Request 33: `{When: 388423, Kind: 15, Args: [457, "41"]}`
- Request 34: `{Kind: 4, When: 388444, Args: [1048, "class", ...]}`
- Request 35: `{When: 388567, Kind: 14, Args: [457, "4111"]}`
- Request 36: `{When: 388670, Kind: 18, Args: [1047, "4111"]}`
- Request 37: `{When: 388671, Kind: 15, Args: [457, "4111"]}`
- Request 38: `{When: 389375, Kind: 14, Args: [457, "4111"]}`
- Request 39: `{When: 389454, Kind: 18, Args: [1047, "41111"]}`
- Request 40: `{When: 389455, Kind: 15, Args: [457, "41111"]}`
- Request 41: `{When: 389567, Kind: 14, Args: [457, "41111"]}`
- Request 42: `{When: 389630, Kind: 18, Args: [1047, "411111"]}`
- Request 43: `{When: 389631, Kind: 15, Args: [457, "411111"]}`
- Request 44: `{When: 389775, Kind: 14, Args: [49]}`

Web Session Replay

• Questions, suggestions, comments?

- Chicken Little
- Tortoise and hare
- Each of us safer, all of us safer