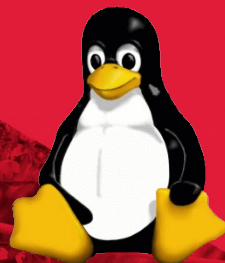




Spectre, Meltdown & Linux

Greg Kroah-Hartman





Greg Kroah-Hartman



Disclaimer

- This talk vastly over-simplifies things
- See notes for full details and resources

<https://github.com/gregkh/presentation-spectre>



Spectre

- Hardware bugs
- Valid code can be “tricked” into exposing sensitive data to attacking programs
- Exploits the “speculative execution” model of modern CPUs
- Many different “variants”
- Is going to be with us for a very long time



Different “Variants”

- 1 – Bounds Check Bypass (BCB)
- 2 – Branch Target Isolation (BTI)
- 3 – Rouge Data Cash Load (RDCL)
- 3a – Rouge System Register Read (RSRE)
- 4 – Speculative Store Bypass (SSB)
- 5 – Lazy FP State Restore (LazyFP)



variant 1 – Bounds check bypass

- Use the kernel to read memory of another process or virtual machine
- Fixed by core kernel changes
- Fixed by lots of driver changes



variant 1 – vulnerable code

```
int load_array(int *array, unsigned int user_value)
{
    if (user_value >= MAX_ARRAY_ELEMS)
        return 0;

    return array[user_value];
}
```



variant 1 – fixed code

```
int load_array(int *array, unsigned int user_value)
{
    if (user_value >= MAX_ARRAY_ELEMS)
        return 0;

    user_value = array_index_nospec(user_value,
                                    MAX_ARRAY_ELEMS);
    return array[user_value];
}
```




variant 1 – Fix dates*

- x86
 - 4.14.14 17 January 2018
 - 4.9.77 17 January 2018
 - 4.4.113 23 January 2018
- ARM
 - 4.15.4 17 February 2018
 - 4.14.21 22 February 2018



*Fixes keep coming

- These are the “first fixed” dates.
- Later kernels get more fixes and improvements
- Keep updating your kernel!



variant 1 – Fix dates again

- x86
 - 4.16.11 22 May 2018
 - 4.14.43 22 May 2018
 - 4.9.102 22 May 2018
- ARM
 - 4.16 1 April 2018
 - 4.9.95 20 April 2018



variant 2 – Branch target injection

- Abuses the CPU branch predictor
- Read data from kernel or other virtual machine
- Fixed by both kernel and microcode updates
- “[retpoline](#)”



variant 2 – Fix dates*

- x86
 - 4.15.9 11 March 2018
 - 4.14.26 11 March 2018
 - 4.9.87 11 March 2018
 - 4.4.121 11 March 2018

*More fixes and optimizations happened in later kernels



Meltdown

- Spectre variant “3”
- Read kernel data from userspace
- Fixed with “page table isolation” kernel changes (Kaiser)
- Slows down enter/exit of the kernel
- Implemented differently for different kernel releases and distros



Meltdown – fix dates

- x86
 - 4.14.11 02 January 2018
 - 4.9.75 05 January 2018
 - 4.4.110 05 January 2018
- ARM
 - 4.15.4 17 February 2018
 - 4.14.20 17 February 2018
 - 4.9.93 08 April 2018



variant 3a – Rouge system register read

- Abuses the reading of system registers
- Read data from kernel or other virtual machine
- Kernel fix for Meltdown solves this problem



variant 4 – Speculative Store Bypass

- Can execute and read beyond what is expected.
- Read data from kernel or other virtual machine
- Minor kernel changes
- Microcode update required for full protection



variant 4 – Speculative Store Bypass

- x86
 - 4.16.11 22 May 2018
 - 4.14.43 22 May 2018
 - 4.9.102 22 May 2018



variant 1 – Bounds check bypass

- Use the kernel to read memory of another process or virtual machine
- Fixed by core kernel changes
- Fixed by lots of driver changes

Click to edit title

- Click to edit text
 - Second level
 - Third level
 - Fourth level
 - » Fifth level

Timeline

- Publicly announced January 3, 2018
- First reported by Google to Intel in July, 2017
 - Independently discovered by others afterward
- Very long embargo
- 3 distros notified in September 2017
- Some kernel developers learned about Meltdown in October 2017
- Kernel security team was never notified

Meltdown fix dates*

- x86
 - 4.14.11 02 January 2018
 - 4.9.75 05 January 2018
 - 4.4.110 05 January 2018
- ARM
 - 4.15.11 17 Febuary 2018
 - 4.14.20 17 Febuary 2018

Click to edit title

- Click to edit text
 - Second level
 - Third level
 - Fourth level
 - » Fifth level



THE LINUX FOUNDATION



AUTOMOTIVE
LINUX SUMMIT

