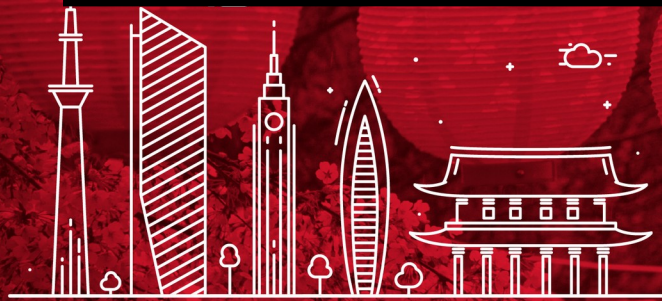
THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
JAPAN

AUTOMOTIVE
LINUX SUMMIT

Spectre, Meltdown & Linux

Greg Kroah-Hartman



THE LINUX FOUNDATION

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
JAPAN

AUTOMOTIVE
LINUX SUMMIT

Greg Kroah-Hartman

THE LINUX FOUNDATION

Spectre

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

Spectre variants

- 1 – bounds check bypass
- 2 – branch target isolation
- 3 – rouge data cash load
- 3a – rouge system register read
- 4 – speculative store bypass
- 5 – Lazy FP state restore

Meltdown

- Spectre varient “3”
- Read kernel data from userspace
- Fixed with “page table isolation” kernel changes (Kaiser)
- Slows down enter/exit of the kernel
  - I/O heavy loads are hit hard
- Implemented differently for different kernel releases and distros

Click to edit title

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

Spectre sample code - vulnerable

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

      return array[user_value];
}
```

Spectre sample code - fixed

```
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];
}
```

Timeline

- Publically announced January 3, 2018
- First reported by Google to Intel in July, 2017
  - Independantly discovered by others afterward
- Very long embargo
- 3 distros notified in September 2017
- Some kernel developers learned about Meltown 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

OPEN SOURCE SUMMIT JAPAN

AUTOMOTIVE LINUX SUMMIT

THE LINUX FOUNDATION