Tower Probe Race Condition

PRESENTED BY ROBERT BLAND & TYLER TOWNSEND

Problem: CVE-2017-15102

“The tower_probe function in drivers/usb/misc/legousbtower.c in the Linux kernel before 4.8.1 allows local users (who are physically proximate for inserting a crafted USB device) to gain privileges by leveraging a write-what-where condition that occurs after a race condition and a NULL pointer dereference.”

What is a Tower_Probe?

- Tower_Probe is a function that exists within the legousbtower driver
  - Legousbtower driver provides support for LegoZ Mindstorms USB IR Tower
- The Tower_Probe function is responsible for both registering the usb device and for confirming the devices firmware board ID
- If there is an error in confirming firmware ID then Tower_Probe will call Tower_Delete (Important)

What is Legousbtower?

Device driver built for Lego USB IR Device

- First released in 2001
- Added to the linux kernel in version 2.6.1

Problem at Hand (Assumptions)

We must assume a few the attacker has done the following:

1. The attacker has a forged USB device with an invalid firmware ID
2. Will do a write operation using this device
3. Will delay the call to Tower_Delete until the write operation starts

Problem at Hand (Effects)

What can the attacker do now that we have this scenario?

- Now possible to create a race condition between the write operation and Tower_Probe executing Tower_Delete
- The race condition is possible because the device is registered before confirming the firmware ID
  - Allows attacker to perform global reads/writes before calling the ID confirm operation
- Bad firmware ID causes the ID confirm operation inside the Tower_Probe to call Tower_Delete

Problem (Picture)

Lines 5-21 is when Tower_Probe registers the device

We stall before calling usb_control_msg on line 24

Attacker concurrently executes a read/write operation and then stop stalling to allow for the Tower_Delete call

```
1  @@ -886,24 +886,6 @@ static int tower_probe (struct usb_interface *
     interface, const struct usb_device
2    dev->interrupt_in_interval = interrupt_in_interval ?
       interrupt_in_interval : dev->interrupt_in_endpoint->bInterval;
3    dev->interrupt_out_interval = interrupt_out_interval ?
       interrupt_out_interval : dev->interrupt_out_endpoint->bInterval
       ;
4
5    /* we can register the device now, as it is ready */
6    usb_set_intfdata (interface, dev);
7
8    retval = usb_register_dev (interface, &tower_class);
9
10   if (retval) {
11     /* something prevented us from registering this driver */
12     dev_err(idev, "Not able to get a minor for this device.\n");
13     usb_set_intfdata (interface, NULL);
14     goto error;
15   }
16   dev->minor = interface->minor;
17
18   /* let the user know what node this device is now attached to */
19   dev_info(&interface->dev, "LEGO USB Tower #%d now attached to
       major "
20      "%d minor %d\n", (dev->minor - LEGO_USB_TOWER_MINOR_BASE),
21      USB_MAJOR, dev->minor);
22
23   /* get the firmware version and log it */
24   result = usb_control_msg (udev,
25           usb_rcvctrlpipe(udev, 0),
26 @@ -924,6 +906,23 @@ static int tower_probe (struct usb_interface *
     interface, const struct usb_device
27      get_version_reply.minor,
28      le16_to_cpu(get_version_reply.build_no));
29
30  exit:
31   return retval;
```

Result

```
291  static inline void tower_delete (struct lego_usb_tower *dev)
292  {
293          tower_abort_transfers (dev);
294
295          /* free data structures */
296          usb_free_urb(dev->interrupt_in_urb);
297          usb_free_urb(dev->interrupt_out_urb);
298          kfree (dev->read_buffer);
299          kfree (dev->interrupt_in_buffer);
300          kfree (dev->interrupt_out_buffer);
301          kfree (dev);
302  }
```

```
681          if (copy_from_user (dev->interrupt_out_buffer, buffer, bytes_to_write)) {
682                  retval = -EFAULT;
683                  goto unlock_exit;
684          }
685
686          /* send off the urb */
687          usb_fill_int_urb(dev->interrupt_out_urb,
688                           dev->udev,
689                           usb_sndintpipe(dev->udev, dev->interrupt_out_endpoint->bEndpointAddress),
690                           dev->interrupt_out_buffer,
691                           bytes_to_write,
692                           tower_interrupt_out_callback,
693                           dev,
694                           dev->interrupt_out_interval);
695
696          dev->interrupt_out_busy = 1;
697          wmb();
698
699          retval = usb_submit_urb (dev->interrupt_out_urb, GFP_KERNEL);
700          if (retval) {
701                  dev->interrupt_out_busy = 0;
702                  dev_err(&dev->udev->dev,
703                          "Couldn't submit interrupt_out_urb %d\n", retval);
704                  goto unlock_exit;
705          }
706          retval = bytes_to_write;
707
708  unlock_exit:
709          /* unlock the device */
710          mutex_unlock(&dev->lock);
711
712  exit:
713          return retval;
```

Delete frees dev->interrupt_out_urb (Line 297)
Write operation then has a NULL pointer dereference and causes a write-what-where condition

Result (Part 2)

The following is what occurs:

1. Exposes a write-what-where condition by remapping dev->interrupt_out_buffer
   - Write-what-where condition is when the attacker can write an arbitrary value to an arbitrary location, usually caused by overflow
2. Leads to local privilege escalation and allows the attacker to execute their own malicious code

Note: This is only possible if 0 is mappable on the Linux machine and the linux machine kernel has to be a version between 2.6.1x and 4.8.0x

Solution

Solution is fairly simple

- It’s only a restructuring of the already existing code in Tower_Probe
- Instead of registering the device before confirming board’s ID we register it after the confirmation
- Makes stalling meaningless by eliminating the possibility of a read/write operation to happen concurrently with a Tower_Delete

Solution (Picture)

- What to know about the picture:
  - Negative signs are the lines of code that we delete
  - Positive signs are the lines of code we add
- Note that we cut and pasted where we register our device to be after we check the firmware ID

```
@@ -886,24 +886,6 @@ static int tower_probe (struct usb_interface *
    interface, const struct usb_device
  dev->interrupt_in_interval = interrupt_in_interval ?
    interrupt_in_interval : dev->interrupt_in_endpoint->bInterval;
  dev->interrupt_out_interval = interrupt_out_interval ?
    interrupt_out_interval : dev->interrupt_out_endpoint->bInterval
    ;

- /* we can register the device now, as it is ready */
- usb_set_intfdata (interface, dev);
-
- retval = usb_register_dev (interface, &tower_class);
-
- if (retval) {
-   /* something prevented us from registering this driver */
-   dev_err(idev, "Not able to get a minor for this device.\n");
-   usb_set_intfdata (interface, NULL);
-   goto error;
- }
- dev->minor = interface->minor;
-
- /* let the user know what node this device is now attached to */
- dev_info(&interface->dev, "LEGO USB Tower #%d now attached to
    major "
-    "%d minor %d\n", (dev->minor - LEGO_USB_TOWER_MINOR_BASE),
-    USB_MAJOR, dev->minor);
-
  /* get the firmware version and log it */
  result = usb_control_msg (udev,
          usb_rcvctrlpipe(udev, 0),
@@ -924,6 +906,23 @@ static int tower_probe (struct usb_interface *
    interface, const struct usb_device
     get_version_reply.minor,
     le16_to_cpu(get_version_reply.build_no));

+ /* we can register the device now, as it is ready */
+ usb_set_intfdata (interface, dev);
+
+ retval = usb_register_dev (interface, &tower_class);
+
+ if (retval) {
+   /* something prevented us from registering this driver */
+   dev_err(idev, "Not able to get a minor for this device.\n");
+   usb_set_intfdata (interface, NULL);
+   goto error;
+ }
+ dev->minor = interface->minor;
+
+ /* let the user know what node this device is now attached to */
+ dev_info(&interface->dev, "LEGO USB Tower #%d now attached to
    major "
+    "%d minor %d\n", (dev->minor - LEGO_USB_TOWER_MINOR_BASE),
+    USB_MAJOR, dev->minor);

 exit:
  return retval;
```

Concurrency and Synchronization

What does this have to do with concurrency? There was no locks or compare-and-swaps shown in the code, so how does it relate to it?

- This vulnerability is only present with concurrent operations
  - A sequential ordering would cause the stalling to be pointless and eliminates race conditions
  - Impossible to do a read/write operation and call Tower_Delete
- Exemplifies how race conditions in concurrent operations can cause security vulnerabilities given the right conditions
  - Conditions are very specific, but a vulnerability is still a security risk that has to be addressed
  - If it can happen once then it can be exploited repeatedly

References

- Github
  - https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=2fae9e5a7babada041e2e161699ade2447a01989
- Link to vulnerability history
  - https://nvd.nist.gov/vuln/detail/CVE-2017-15102#vulnCurrentDescriptionTitle
- LegoUSB Project website
  - http://legousb.sourceforge.net/legousbtower/index.shtml

Driver_Override Race Condtion

PRESENTED BY ROBERT BLAND & TYLER TOWNSEND

Problem: CVE-2017-12146 Detail

“The driver_override implementation in drivers/base/platform.c in the Linux kernel before 4.12.1 allows local users to gain privileges by leveraging a race condition between a read operation and a store operation that involve different overrides.”

Driver_Override Overview

- Devices need drivers to connect to O.S.
- Drivers for these devices are need
- The driver_override field is implemented in struct platform_device
  - Allows the driver for a device to be specified to override standard binding protocol
  - Executed by writing a string to the driver_override file
- Two functions
  - Driver_override_store(): write driver_override
  - Driver_override_show(): read driver_override

Problem

```
static ssize_t driver_override_store(struct device *dev,
                    struct device_attribute *attr,
                    const char *buf, size_t count)
{
  struct platform_device *pdev = to_platform_device(dev);
  char *driver_override, *old = pdev->driver_override, *cp;

  if (count > PATH_MAX) return -EINVAL;
  driver_override = kstrndup(buf, count, GFP_KERNEL);

  if (!driver_override) return -ENOMEM;
  cp = strchr(driver_override, '\n');
  if (cp) *cp = '\0';

  if (strlen(driver_override)) {
    pdev->driver_override = driver_override;
  } else {
    kfree(driver_override);
    pdev->driver_override = NULL;
  }

  kfree(old);
  return count;
}
```

```
static ssize_t driver_override_show(struct device *dev,
                    struct device_attribute *attr, char *buf)
{
  struct platform_device *pdev = to_platform_device(dev);
  return sprintf(buf, "%s\n", pdev->driver_override);
}
```

Problem

```
static ssize_t driver_override_store(struct device *dev,
                    struct device_attribute *attr,
                    const char *buf, size_t count)
{
  struct platform_device *pdev = to_platform_device(dev);
  char *driver_override, *old = pdev->driver_override, *cp;

  if (count > PATH_MAX) return -EINVAL;
  driver_override = kstrndup(buf, count, GFP_KERNEL);

  if (!driver_override) return -ENOMEM;
  cp = strchr(driver_override, '\n');
  if (cp) *cp = '\0';

  if (strlen(driver_override)) {
    pdev->driver_override = driver_override;
  } else {
    kfree(driver_override);
    pdev->driver_override = NULL;
  }

  kfree(old);
  return count;
}
```

```
static ssize_t driver_override_show(struct device *dev,
                    struct device_attribute *attr, char *buf)
{
  struct platform_device *pdev = to_platform_device(dev);
  return sprintf(buf, "%s\n", pdev->driver_override);
}
```

Execution

T1: Store

```
old = pdev->driver_override
pdev->driver_override
        =driver_overide
kfree(old)
```

1

T2: Show

```
sprintf(buf, “%s\n”,
        pdev->driver_override)
```

2

Execution

T1: Store

old = pdev->driver_override

pdev->driver_override

=driver_overide

kfree(old)

T2: Show

sprintf(buf, “%s\n”,

pdev->driver_override)

Execution

T1: Store

old = pdev->driver_override

pdev->driver_override

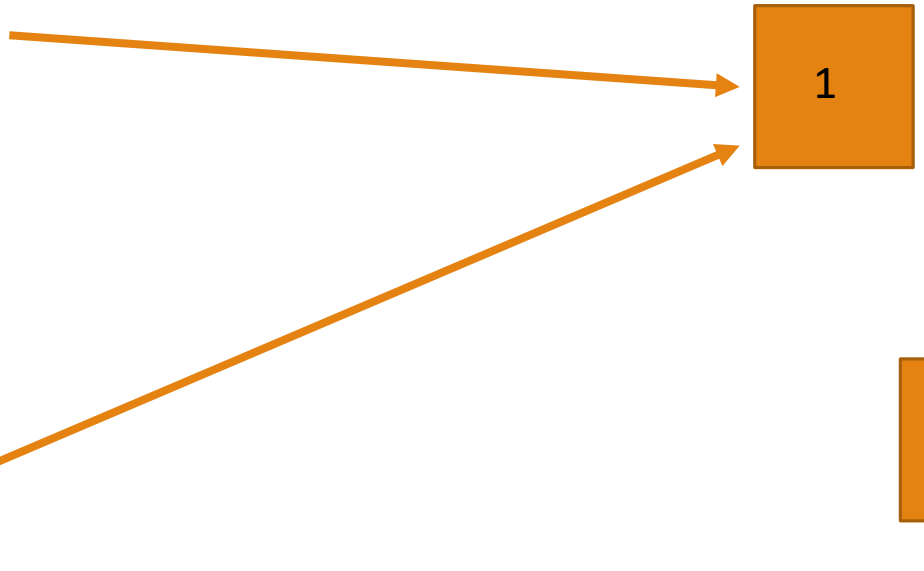
=driver_overide

kfree(old)

T2: Show

sprintf(buf, “%s\n”,

pdev->driver_override)



Execution

T1: Store

old = pdev->driver_override

pdev->driver_override

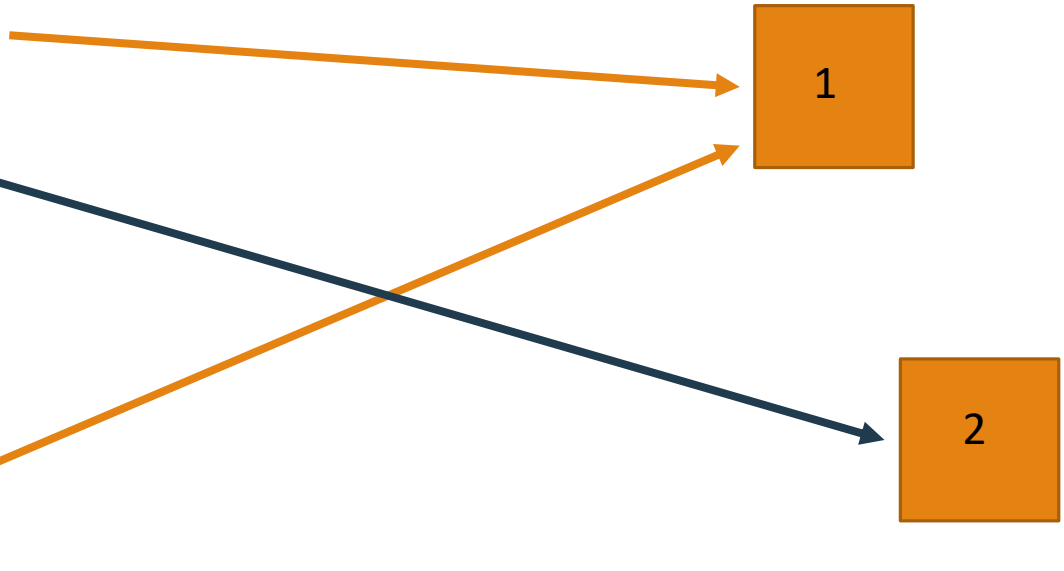
=driver_overide

kfree(old)

T2: Show

sprintf(buf, “%s\n”,

pdev->driver_override)



Execution

T1: Store

old = pdev->driver_override

pdev->driver_override

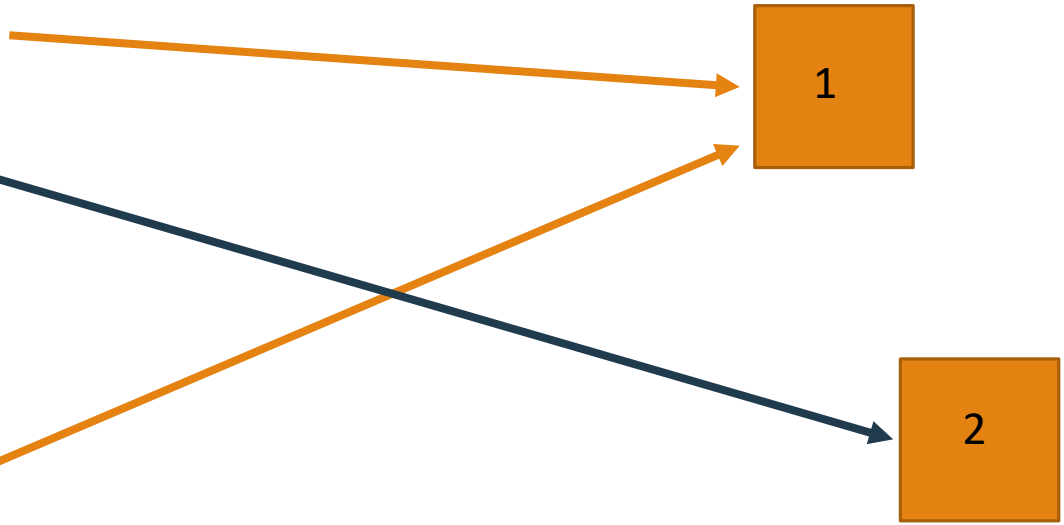
=driver_overide

kfree(old)

T2: Show

sprintf(buf, “%s\n”,

pdev->driver_override)



Execution

T1: Store

old = pdev->driver_override

pdev->driver_override

=driver_overide

kfree(old)

T2: Show

sprintf(buf, “%s\n”,

pdev->driver_override)

2

Solution

- Introduce locks to protect shared data

```
driver_override_store(dev):
        pdev = to_platform_dev(dev)
        …
        lock(dev)
        old = pdev->driver_override
        update(pdev->driver_override)
        unlock(dev)

        kfree(old)
        return count
```

```
driver_override_show(dev, buffer):
        pdev = to_platform_dev(dev)
        lock (dev)
        len = sprintf(buffer, “%s\n”, pdev->driver_override)
        unlock(dev)
        return len
```

Concurrency and Synchronization

- Adding locks allows read and write to complete, atomically.
- Ensures that the data written to buffer is not corrupted during execution
  - If buffer is written to, then a similar thread has either completed overwriting or is blocking for resource
- Also synchronization between multiple stores()
  - Only 1 thread may write pdev->driver_override
  - Only 1 thread may free memory pointed to by old.

References

- Source Code
  - https://elixir.bootlin.com/linux/v4.12.14/source/drivers/base/platform.c
- Vulnerability Database
  - https://vuldb.com/?id.106296
- Patch to implement Override_Driver
  - https://www.redhat.com/archives/libvir-list/2014-April/msg00382.html
- Patch to Fix Race Condition
  - https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6265539776a0810b7ce6398c27866ddb9c6bd154