It rather involved being on the other side of this airtight hatchway: Passing invalid parameters from kernel mode to another kernel-mode function corrupts the kernel (who knew?)

devblogs.microsoft.com/oldnewthing/20180424-00

April 24, 2018

Raymond Chen

A customer reported a vulnerability in a kernel function, let's call it `kfunc`.

> The kernel-mode `kfunc` function doesn't validate any of the pointers passed to it. As a result, you can pass anything you want as the output pointer, and it will blindly try to write to it. If you pass null, you will crash the kernel. Or if you pass a pointer to memory you want to corrupt, you can corrupt an arbitrary 4-byte value.
>
> Maybe I can find a way to pass an invalid parameter from user space all the way down to the `kfunc` function.
>
> Please contact us soon regarding this issue!

Okay, first things first. In the first paragraph, there is no elevation. The kernel-mode `kfunc` function is callable only from kernel mode. The caller is in kernel mode, and it is tricking a kernel mode function into writing to an arbitrary memory location. But so what? The caller could just save itself the trouble of using `kfunc` as the middle man and just corrupt the memory directly. In other words, instead of

```
void attack_the_kfunc()
{
 kfunc(crazy_pointer_value);
}
```

you can just do

```
void attack_the_kfunc()
{
 *crazy_pointer_value = 42;
}
```

This is even more powerful, because not only do you get to corrupt the memory at `crazy_pointer_value`, you even get to pick what value to corrupt it with!

Now, if there were a way to call the `kfunc` function with parameters controlled by user mode, then you would be onto something.

Which leads us to the next paragraph, which boils down to "Maybe there is a way to call the `kfunc` function with parameters controlled by user mode." In other words, the second paragraph says, "Maybe I can find a vulnerability."

Yeah, maybe you can find a vulnerability. Let us know if you do.

But so far, you haven't found a vulnerability. All you've said is "Maybe there is somebody who is doing a bad thing."

"Industrial paper-cutting machines are dangerous and expensive. We keep the paper-cutting machine in a special room, and only people who have gone through training are allowed in the room. Maybe there is a way to get somebody who has access to the special room to put an unauthorized object in the paper-cutting machine and damage it."

Yeah, maybe. If you find such a person, let us know. Because they're in a lot of trouble.

Raymond Chen

Follow