It rather involved being on the other side of this airtight hatchway: Producing malicious data in a kernel driver

devblogs.microsoft.com/oldnewthing/20211207-00

December 7, 2021

Raymond Chen

A security vulnerability report went something like this:

> We have found a vulnerability in the `LogXyz` function. If the packet being logged contains malicious field lengths, the function can read past the end of the buffer and log data from its process space, resulting in information disclosure. Attached is a sample driver that triggers the overflow.

Okay, that sounds bad. This is the sort of thing that led to Heartbleed.

But a closer look at the `LogXyz` function shows that the packet it is logging came from a driver. So this attack presupposes that a malicious driver has been installed on the system.

If you have a malicious driver on your system, you have bigger problems than a buffer overflow in a logging function.

What we have here is a bug, but not a security vulnerability. The `LogXyz` function should be more resilient to malformed data, but any such malformed data came from kernel mode, which already has the power to do anything it wants to user mode. The driver could just access the `LogXyz` function's memory directly and get whatever it wants, no need to trick it into writing the information to a log (and then having to go dig it out of the log).

Raymond Chen

Follow