When people ask for security holes as features: Privileged execution

devblogs.microsoft.com/oldnewthing/20090924-00

September 24, 2009

Raymond Chen

A customer wanted to know if there was a way to execute privileged instructions without having to write a driver. “I just need to execute a few instructions, and writing a driver would be overkill since it’s only three instructions. Is there a way I can execute these privileged instructions without a driver?” The whole point of having a class of modules called drivers is to prevent somebody from doing exactly what you’re asking for. Only drivers can execute privileged instructions; that’s why they’re called privileged instructions. “Yeah, but I just need three instructions. Do I have to write a whole driver just for those three instructions?” Even just one instruction can pwnz0r a machine. You have to be a driver in order to have that much power over the computer. “Maybe there’s a driver somebody has already written that I can give the instructions to, and it’ll execute them for me?” If somebody has written a driver which is designed to execute arbitrary instructions handed to it from user-mode, that person needs to be taken outside and beaten. It’s one thing to have a bug that permits arbitrary code execution, but to have it as the *purpose* of your driver? Think of writing a driver as having access to the secure area of a nuclear power plant. People have to be granted the appropriate security clearance before they are allowed into enter the control room. If you want to get into the control room of the nuclear power plant, you’ll have to apply for security clearance. “But that’s so much work. I just need to go in and change a few settings on the control panel.” Dude, that’s why you’re not allowed in, so you won’t change those settings! Your options are either to get security clearance yourself, or convince somebody with security clearance to change the settings for you. “Well, do you know somebody who does have security clearance who will change any settings I tell him to?”

Gosh, I sure hope not.

Raymond Chen

Follow