It rather involved being on the other side of this airtight hatchway: Elevation from Administrator to SYSTEM

devblogs.microsoft.com/oldnewthing/20150923-00

September 23, 2015

Raymond Chen

A security vulnerability report arrived that took the following form:

> I have discovered a critical security vulnerability in Windows which I intend to present at the XYZ conference. It allows any user with administrator privileges to perform operation Q, something that should be available only to SYSTEM.

I think you know how this story ends. If you have administrator privileges, then you are already on the other side of the airtight hatchway. That you can use administrator privileges to pwn the machine is not interesting, because by virtue of being an administrator *you already pwn the machine*.

There is formally a distinction between Administrator and SYSTEM, seeing as they are some things which are ACL'd so that SYSTEM can do them and not arbitrary adminitrators, but that distinction is formal and not practical. An administrator who wanted to get some code running as SYSTEM could install a service that runs as SYSTEM. Or use Debug Privilege to take over a process (say, a service) running as SYSTEM. Or simply open a command prompt as SYSTEM and go to town. No need to go through the complex operation Q to get SYSTEM access.

So yes, a user with administrator privileges can use operation Q to do things that are normally limited to SYSTEM. But so what? Users with administrator privileges already have plenty of easier ways of doing things that are normally limited to SYSTEM. The distinction between the SYSTEM and Administrator accounts is a roadblock to make it harder to mess up your system by mistake. You can still mess up your system, but you have to try harder.

Before dismissing these reports, you have to verify that the attack is effective only against the current machine. In other words, that obtaining administrator privileges on the computer gets you nothing more than administrator privileges on the computer. And in this case, that was true. The attack described gives the user access to the local machine, but had no effect on other machines.

Raymond Chen

Follow