It rather involved being on the other side of this airtight hatchway: Creating problematic files in a directory that requires administrative access

devblogs.microsoft.com/oldnewthing/20130912-00

September 12, 2013

Raymond Chen

A security vulnerability report came in that said, "If you create a file with ‹specific name› in ‹specific directory›, then ‹denial of service› happens the next time somebody does ‹specific operation›, and the machine must be rebooted." Yes, it's true that creating that specific file in the very specific directory can sow the seeds for a denial of service, and thanks for pointing that out, and we'll fix the problem, but this is not a security vulnerability because ‹specific directory› is writable only by administrators. In other words, in order to carry out this attack, you need to gain administrator privileges. But if you have administrator privileges, then you're already on the other side of the airtight hatchway. If your goal was to attack the machine by triggering a denial of service that forces a reboot, then just use your administrator privileges to shut down the computer! No need to go about this clever roundabout way of triggering a denial of service when you can take the direct approach. It's like saying, "If you go to the master control panel and throw all the auxiliary switches, then the circuit breaker will trip, and the plant will shut down. This is a security vulnerability in the master control panel."

First of all, thanks for letting us know about the problem with the master control panel. We'll have our engineers look it. But the master control panel is in the control room, and you need security clearance to get into the control room in the first place. And if somebody with security clearance wants to shut down the plant, then instead of throwing all the auxiliary switches to trigger a shutdown, then can simply hit the *emergency shutdown* button.

Raymond Chen

Follow