It rather involved being on the other side of this airtight hatchway: System corruption caused by an administrator

devblogs.microsoft.com/oldnewthing/20240404-00

April 4, 2024

Raymond Chen

A security vulnerability report came in that went roughly like this:

> I have found a permanent denial of service vulnerability in Windows. If you modify this administrative setting (directly via regedit, not via the user interface) to have a specific corrupted value, then when the system boots up, it will use this corrupted value and corrupt the operating system itself, rendering the system unusable. Modifying the setting back to its original value does not repair the problem. The system is permanently corrupted and must be reinstalled. I am requesting a bounty for this report.

This is a fairly cut-and-dried case of "It rather involved being on the other side of this airtight hatchway": Modifying the setting in question requires administrator privilege, and it's hardly a surprise that an administrator can render a system inoperable.

Breaking the system by corrupting an administrative setting is just style points. If you are an administrator and want to render a system inoperable, just delete everything in sight, starting with all the files in `C:\Windows\System32`. Delete anything that isn't nailed down, and then go get your crowbar (also known as "Take Ownership" privilege) and pry up even the things that are nailed down.[1] No need to get all clever with crafting a corrupted setting.

Now, if the corruption of the setting could be triggered by means that don't require administrator privileges, then you would have found something. But as it stands, it requires administrator permissions to perform this attack, so you're starting on the other side of the airtight hatchway.

The finder argued that it is a security flaw that the system doesn't prevent administrators from corrupting the setting. For example, there are some registry keys in the system that are protected from accidental corruption by making them read-only even to administrators. But these are merely safety measures, not security boundaries. It's like putting a cover over the emergency shutoff switch in the control room: The cover doesn't prevent anyone in the control room from pulling the switch. It merely prevents them from pulling the switch

accidentally. If somebody with access to the control room really wants to pull the switch or corrupt the registry key, they can do it: They can lift the cover or take ownership of the key and grant themselves full access.

The finder also argued that the system should protect itself from installers that corrupt the setting. But if an installer can corrupt the setting, that means that the installer is running with administrator privileges, so it already can do anything it wants. And that includes removing the corruption protection and rendering the system unusable.

Mind you, preventing administrators or installers from inadvertently corrupting the setting sounds like a reasonable *safety* measure, and the system already does part of that by showing only non-corrupted options in the administrator user interface. And having the system recognize a corrupted value and stop itself before causing any permanent damage is a reasonable *reliability* measure, so thanks for pointing out the issue. But it's not a security issue. You can't protect against an administrator who intentionally decides to mess up their system.

[1] Another idea is to turn on BitLocker and throw away the BitLocker key. Or go into Advanced Recovery and reformat the system volume!