It rather involved being on the other side of the airtight hatchway: Disabling a security feature as an administrator

devblogs.microsoft.com/oldnewthing/20240806-00

August 6, 2024

Raymond Chen

A security vulnerability report claimed that they were able to bypass a security feature in three easy steps:

1. Open Regedit.
2. Go to `HKLM\Software\Microsoft\⟦redacted⟧`.
3. Double-click the `Enabled` registry value and change it from 1 to 0.

The security feature is now disabled!

Well yeah, because you disabled it.

The `Enabled` registry value is in the `HKEY_LOCAL_MACHINE` portion of the registry which by default requires administrator access to modify. In order to carry out this attack, you have to already be an administrator on the system, in which case a much easier way to bypass the security feature is to just go to the Settings UI for the feature and disable it there.

This is cut-and-dried but it's really surprising how often people appear to be concerned that an *administrator* can compromise security.

No really, variations on this non-vulnerability are reported *a lot*. They all boil down to, "I found a security vulnerability: An administrator can disable a security feature!" Sometimes, they even admit it themselves: "You must run the PoC as an administrator." Other times, they confess to not being an expert on the subject: “I am not a security expert, but I can confidently say that I can bypass the security feature using this method.”

Bonus chatter: Here’s another example of a vulnerability report in this category.

> A malicious driver can bypass or disable Windows security features.
>
> Step 1: Open an elevated command prompt.
>
> …

Okay, I’m just going to stop you right there. If your first step is “open an elevated command prompt”, then you don’t need to do all those sneaky things to install the malicious driver in the super-clever way so that it can bypass and disable Windows security features. From the elevated command prompt, you can just disable the security features directly!