It rather involved being on the other side of this airtight hatchway: Messing with somebody’s registry

devblogs.microsoft.com/oldnewthing/20190109-00

January 9, 2019

Raymond Chen

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

> If a user obtains write access to another user’s registry, then the user can make that other user’s life miserable by making the following changes to the victim’s registry. … A proof of concept program is attached which makes the necessary changes to the registry.

While the above statement is true, it doesn’t really say anything interesting either.

- It is possible for users to make their own lives miserable.
- If you get write access to another user’s settings, you can change those settings in a way that makes that user’s life miserable.

The proof of concept program edits keys in the `HKEY_CURRENT_USER` registry hive, so it must be run by the user whose life you are trying to make miserable (or by someone who has permission to make that user’s life miserable).

It is not a security vulnerability that users can make their own lives miserable. If you want to deny yourself access to your own files, or if you want to render parts of your own work environment non-functional, then go ahead. Smash your television set. Take the books from your bookshelf and throw them onto the floor. It’s your television set. They’re your books. If you want to make using them inconvenient or impossible, then that’s your prerogative.

The obstacle to wreaking all this havoc on other users is obtaining write access to their registry. The finder didn’t actually demonstrate how to obtain this; they merely noted that *if* you could obtain such access, then you could make the other user’s life miserable.

Well, yeah. If you have the keys to somebody’s house, you can go in and smash their television set and throw their books on the floor.

But it all hinges on getting the keys to the house.

Until you show how to get access to the other user's registry, you haven't stated anything that isn't already obvious.

Raymond Chen

Follow