Dubious security vulnerability: A program that adds a user to the Administrators group in the usual way

devblogs.microsoft.com/oldnewthing/20181106-00

November 6, 2018

Raymond Chen

A security vulnerability report indicated that Windows was vulnerable to having a user added to the Administrators group. The finder attached a program demonstrating the issue. (To make things more exciting, they characterized the program as “malicious” and the person running it as an “attacker”.)

The finder didn’t include source code, but the program was small enough that it could be reverse-compiled without too much difficulty. The program employs the usual mechanisms for adding a user to the Administrators group. Nothing particularly fancy. Just calling documented functions in documented ways to accomplish the documented effect. When you run the program as a standard user, it fails with *Access denied*, as expected. Only if you run it as an administrator does it succeed in adding a user to the Administrators group.

Which is as things should be.

There didn’t appear to be anything unusual going on here. No security boundary was crossed. Nothing suspicious happened.

The finder explained that this program, when run elevated, adds a user to the Administrators group, and no anti-malware program flagged it as suspicious.

Well yeah, because it’s not suspicious. It does something perfectly legitimate, via perfectly legitimate means, and it doesn’t attempt to subvert any security measures. Indeed, this is the sort of quick little program that you might see in a system administrator’s toolbox.

It’s expected that a program which does nothing suspicious is not flagged as suspicious.

Bonus reading: The Ten Immutable Laws of Security (Version 2.0), specifically law #1: If a bad guy can persuade you to run his program on your computer, it’s not solely your computer anymore.

Raymond Chen

Follow