Dubious security vulnerability: Tricking a program into running non-elevated

devblogs.microsoft.com/oldnewthing/20250609-00/?p=111258

June 9, 2025

Within the span of a week,[1] we received two security vulnerability reports that claimed that you could use the RunAsInvoker compatibility layer to run any program without requiring administrator privileges.

I have pointed out in the past that RunAsInvoker is not a secret, even higher UAC setting, but rather a secret, even *lower* UAC setting. What RunAsInvoker does is suppress any attempt at elevation and force the program to run at the same privilege level as the code that launched it. In particular, if you are launching it from a batch file or command line, the program runs elevated if the batch file or command prompt is elevated, and the program runs unelevated if the batch file or command prompt is unelevated.

The finders breathlessly reported that RunAsInvoked allows them to run any program, even one that would normally prompt for elevation.

Which is true.

But what they failed to notice is that the program that is run with RunAsInvoker does not gain any privileges beyond what you already possessed. Using RunAsInvoker to launch a program from an unelevated command prompt results in an unelevated program. So you haven't gained any privileges. The program is still constrained by what a standard user can do.

The program is running, but not as an administrator. You didn't get an elevation prompt because no elevation occurred.

There is no vulnerability that you can take a program that was intended to be run elevated, and force it to run unelevated. The program might get confused when it tries to do something that requires elevation and get an "access denied" error, but that's not the operating system's problem. The operating system prevented the program from performing privileged operations, just like it's supposed to.

You can look at it this way: Instead of using RunAsInvoker to force the program to run at the same privilege as the invoker, you can in principle just extract all the code from the program, paste it into your own program, and then run your program. (Easier is to load the file into a hex editor and edit the manifest to change the `requestedExecutionLevel` from `requireAdministrator` to `asInvoker`.)

In summary, no security boundary is crossed. An unprivileged user cannot use this technique to gain elevated privileges. This technique allows a user to force a program to run non-elevated, which is not a security issue. In fact, we wish more programs ran non-elevated!

[1]I have noted before other examples of effectively identical security vulnerability reports coming in close succession. I think what's happening is that the issue first appears on a private chat room or forum or something, and then people who are members of the chat or forum stumble over each other trying to report it first to get a bounty or street cred or whatever other currency applies to this subculture.