# Dubious security vulnerability: If I perform this complex series of manual steps, I can crash a program I am running

devblogs.microsoft.com/oldnewthing/20250707-00/?p=111351

July 7, 2025

A security vulnerability report arrived that went roughly like this.

> In *Program X*, click on the triangle icon and hold the mouse down. Drag the triangle icon to the green box in the corner, and while still holding the mouse down, press `Alt`+`F4` to close the window. The program will crash on a null pointer.

It sure looks like you found a bug. But is it a security bug?

Who is the attacker? Who is the victim? What has the attacker gained?

The attacker is presumably the person using the mouse and keyboard to trigger the bug.

The victim is, um, I guess it's the person whose program crashed. But wait, that's the same as the attacker!

What the attacker gained is the ability to prevent the victim from getting work done.

It's unclear how this became "elevation of privilege". A crash on null pointer is typically at most a denial of service. And in this case, the attacker is denying service to himself.

If you want to deny service to yourself, you can just click the × button in the top right corner of the window. There, now you can't use the program!

The report finishes with a claim that if malware could trigger the crash, then the malware could use a crafted input to escalate privileges.

First of all, there's no escalation here. The crash is on a null pointer, not a use-after-free or something else that could be leveraged to gain remote code execution. Furthermore, if malware has the ability to inject input, then they don't need this bug to escalate privileges. They could inject input to run an elevated command prompt and type commands into it!