Dubious security vulnerability: A program does not run correctly if you run it the wrong way

devblogs.microsoft.com/oldnewthing/20250317-00

Shawn Van Ness March 17, 2025

Raymond Chen

Two similar denial of service security vulnerability reports arrived on the same day, and a third a day later. Each one took roughly this form, but with different programs substituted for XYZ.exe.

> If you run the XYZ.exe program from the command prompt, it immediately crashes. This is a denial of service attack against XYZ.exe.

In all of the cases, the XYZ.exe programs are intended to be run in a special way. One is a service executable, and when it calls `ServiceMain` to register itself with the service control manager, the call fails ("Why are you calling me? You're not a service!"), and the program exits with an assertion failure. In the other two cases, the programs are intended to be run as UWP programs, but the finder was executing them outside the AppContainer environment. The programs try to communicate with the UWP execution environment and fail, and they exit with assertion failures.

These assertion failures generate Windows Error Reports so that the problem can be investigated by the respective feature teams. After all, there might be a bug in the way the programs registered themselves to be run in their intended execution environments, so the teams want to investigate how their program got into a bad state.

But that's not the case here. The programs fail to start not because they were registered improperly, but because the weren't even being launched by the intended launcher program in the first place!

This was reported as a denial of service, but it's not clear whose service is being denied.

I think the argument is that since the helper program crashes, the denial of service is that it fails to perform its intended task.

But did you prevent it from performing its intended task?

What you crashed was a copy of the helper program that you yourself created. You didn't have any effect on the copies of the helper program used by the main programs. Those are the ones who actually have an intended purpose. And those copies still work fine.

It's like buying an ambulance and putting the wrong kind of gasoline in it. This damages the ambulance. Is this a denial of service against ambulances?

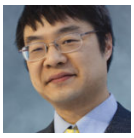
No, this is just a denial of service against *your* ambulance. The ambulances owned by the hospital still work fine.

Now, if you had found a way to get the hospital to put the wrong kind of gasoline in *their* ambulances, then that would be interesting. But so far, this is just a case of destroying your own property. And you are perfectly within your rights to destroy your own property. There is no security vulnerability here.

Bonus chatter: A few weeks later, there was another report very similar to these, but in reverse. "Instead of running the XYZ.exe program from the command prompt or Start menu, run it in a low IL AppContainer. It crashes immediately." Again, it's crashing because you are running it in a way that it was never meant to be run, and in a way that the system never actually tries to run it. Running the program in a low IL AppContainer is nothing the system ever does, nor does the system ever invite the user to do so. Furthermore, the crashing of the program has no impact on anybody else.

Author

Raymond Chen



Raymond has been involved in the evolution of Windows for more than 30 years. In 2003, he began a Web site known as The Old New Thing which has grown in popularity far beyond his wildest imagination, a development which still gives him the heebie-jeebies. The Web site spawned a book, coincidentally also titled The Old New Thing (Addison Wesley 2007). He occasionally appears on the Windows Dev Docs Twitter account to tell stories which convey no useful information.

3 comments

Discussion is closed. Login to edit/delete existing comments.

Newest

- 
  March 18, 2025
  Something I once heard: “Every bug is a security bug, if you report it right.”

  That’s a pro-tip, if you ever want to make sure a bug is triaged as high priority.. “it crashes! this is a denial-of-service vulnerability!”.

- AM
  Arp, Matthew March 18, 2025
  TLDR; I executed your program incorrectly and it crashed

  I’d love to see a new series on your blog of things that turned out to be actual security vulnerabilities.

- KN
  Kalle Niemitalo
  Re executing outside the AppContainer environment, I had assumed that setting the IMAGE_DLL_CHARACTERISTICS_APPCONTAINER bit would cause CreateProcess to return an error if PROC_THREAD_ATTRIBUTE_SECURITY_CAPABILITIES is not provided. But now that I tried it, the process started without an AppContainer anyhow. What’s the real effect of IMAGE_DLL_CHARACTERISTICS_APPCONTAINER?

Stay informed

Get notified when new posts are published.