It rather involved being on the other side of this airtight hatchway: Attacking a user by modifying that user's files

devblogs.microsoft.com/oldnewthing/20230118-00

January 18, 2023

Raymond Chen

A security vulnerability report arrived that went something like this:

> Windows is vulnerable to remote code execution as follows:
>
> - Modify the file `%USERPROFILE%\AppData\Local\Contoso\BlahBlah` and add this line to the PlugIns section.
> - Run the `contoso.exe` program.
> - The `contoso.exe` program loads its configuration from the `BlahBlah` file.
> - When the Contoso app starts, it tries to create a plug-in from the object you configured in PlugIns section, passing the initialization data you also specified in the PlugIns section.
> - By crafting the initialization data, you can get the system-provided object to run a command controlled by the attacker.

That's all very interesting, but what is the vulnerability?

They never said.

The fact that the system-provided object can be induced into executing a command based on its initialization data is not surprising in this case: The initialization data for this particular system-provided object contains a serialized COM object, and deserializing it would naturally end up creating whatever you serialized.

My guess is that the finder was excited that they could modify a file in a way that leads to code execution when a program is run. But let's look at our usual questions.

Who is the attacker?

The attacker is presumably somebody who is able to modify the configuration file.

Who is the victim?

The victim is presumably the user whose configuration file got modified.

What has the attacker gained?

Actually, if you look back at the earlier two questions, you'll see that the attacker and the victim are the same person!

In order to modify a user's files, you have to be that user or an administrator. In all cases, you haven't gained any privileges beyond what you already had. If you're the user, then you are attacking yourself. If you're the administrator, well, it's not interesting that the administrator can attack any user.

If you already had the power to modify the user's files, then you don't need to go to all the work of editing an obscure configuration file for a program the user might not even run. Just drop a batch file in the user's Startup folder.