It rather involved being on the other side of this airtight hatchway: Gaining code execution from a Trojan horse

devblogs.microsoft.com/oldnewthing/20230103-00

January 3, 2023

Raymond Chen

A security vulnerability report arrived that went roughly like this:

> The Xyz object can be used to execute arbitrary command lines.
>
> - `LoadLibrary(L"xyz.dll");`
> - `GetProcAddress` for `DllGetClassObject`.
> - Call `DllGetClassObject` with `CLSID_Xyz` and `IID_IXyz`.
> - From the resulting object, call `IXyz::Initialize`, and then `IXyz::Execute`.

So far, we don't have any statement of vulnerability. Sure, the Xyz object can be used to execute arbitrary command lines, but how is that a security vulnerability?

We asked the finder some questions to clarify the nature of the alleged vulnerability.

> Q: What is the attack vector?
>
> A: The attack vector is a Trojan horse executable. The victim needs to double-click the executable, which triggers the exploit.
>
> Q: Is there elevation of privilege?
>
> A: Not at this time.
>
> Q: Is this remote code execution.
>
> A: Essentially, it is not. The exploit must be downloaded to the victim machine in order to proceed with the attack.
>
> Q: As a result of this exploit, what can the attacker do that they couldn't do without this issue?
>
> A: I don't know. I am not a professional attacker. The main attack technique is as described in the original report. I think I explained it like this.

What we have is another case of if I can trick you into running my program, then I have gained code execution, also known jokingly as MS07-052: Code execution leads to code execution.

If you have gained sufficient trust with the victim that they will run any program you give them, then you don't need the Xyz object in order to launch arbitrary command lines. You already have arbitrary code execution: That's even better than command line execution! You don't need to find an existing program that does whatever bad thing you want to do; you can just make your custom program do that bad thing directly.

Tying up some loose ends: The command line passed to `IXyz::Execute` runs with the same privilege as the caller, so there is no elevation of privilege.

Bonus chatter: Not long afterward, we received the following security vulnerability report:

> Download and run the following script. It deletes all your files. If run as an administrator, it can delete operating system files.

That's nice, but there is no security vulnerability yet. The script can delete only files that the user has permission to delete. In a way, you can say that the script "unlocks the user's full file deletion potential".

If the point of the attack is that the user can be tricked into deleting all their files by running this suspicious script, well, that's not particularly surprising. If you can trick a user into running a suspicious script, then you have effectively tricked them into granting you full access to their account, and it's not surprising that you can delete all their files.

Raymond Chen

Follow