Dubious security vulnerability: Luring somebody into your lair

devblogs.microsoft.com/oldnewthing/20150527-00

May 27, 2015

Raymond Chen

A security report was received that went something like this:

> The XYZ application does not load its DLLs securely. Create a directory, say, `C:\Vulnerable`, and copy `XYZ.EXE` and a rogue copy of `ABC.DLL` in that directory. When `C:\Vulnerable\XYZ.EXE` is run, the XYZ program will load the rogue DLL instead of the official copy in the System32 directory. This is a security flaw in the XYZ program.

Recall that the directory is the application bundle, The fact that the `XYZ.EXE` program loads ABC.DLL from the application directory rather than the System32 directory is not surprising because the ABC.DLL has been placed inside the `XYZ.EXE` program's trusted circle.

But what is the security flaw, exactly?

Let's identify the attacker, the victim, and the attack scenario.

The attacker is the person who created the directory with the copy of `XYZ.EXE` and the rogue `ABC.DLL`.

The victim is whatever poor sap runs the `XYZ.EXE` program from the custom directory instead of from its normal location.

The attack scenario is

- Attacker creates a directory, say, `C:\Vulnerable`.
- `copy C:\Windows\System32\XYZ.EXE C:\Vulnerable\XYZ.EXE`
- `copy rogue.dll C:\Vulnerable\ABC.DLL`
- Convince a victim to run `C:\Vulnerable\XYZ.EXE`.

When the victim runs `C:\Vulnerable\XYZ.EXE`, the rogue DLL gets loaded, and the victim is pwned.

But the victim was already pwned even before getting to that point! Because the victim ran `C:\Vulnerable\XYZ.EXE`.

A much simpler attack is to do this:

- Attacker creates a directory, say, `C:\Vulnerable`.
- `copy pwned.exe C:\Vulnerable\XYZ.EXE`
- Convince a victim to run `C:\Vulnerable\XYZ.EXE`.

The rogue `ABC.DLL` is immaterial. All it does is crank up the degree of difficulty without changing the fundamental issue: If you can trick a user into running a program you control, then the user is pwned.

This is another case of if I can run an arbitrary program, then I can do arbitrary things, also known as MS07-052: Code execution results in code execution.

Note that the real copy of `XYZ.EXE` in the System32 directory is unaffected. The attack doesn't affect users which run the real copy. And since `C:\Vulnerable` isn't on the default `PATH`, the only way to get somebody to run the rogue copy is to trick them into running the wrong copy.

It's like saying that there's a security flaw in Anna Kournikova because people can create things that look like Anna Kournikova and trick victims into running it.

Raymond Chen

Follow