Starting on the other side of the airtight hatchway: Attacking the batch file parser

devblogs.microsoft.com/oldnewthing/20220627-00

June 27, 2022

Raymond Chen

A security vulnerability report arrived saying that they were able to launch a denial of service against the Windows command prompt by executing a batch file with specific malformed command line that confused the parser.

That's great, you found a bug in the command line's parser that you can demonstrate with a batch file. Definitely a bug. But is it a security vulnerability?

We go through the usual questions: Who is the attacker? Who is the victim? What has the attacker gained?

One scenario is that the attacker sits at a command line and types the malformed command line that crashes the command prompt. But in this case, the attacker is attacking himself. If he wanted to crash the command prompt, he could just close it!

Another scenario is that an attacker convinces a naïve user to type the specific malformed command line and cause their command prompt to crash. Equivalently, an attacker tricks a naïve user into downloading and running a batch file that contains the specific malformed command line.

In both cases, the attacker has, via social engineering, gained control over the victim's command prompt. If they wanted to use that to crash the command prompt, they can accomplish it with a lot less typing by saying "Now type the letters E-X-I-T, and then hit Enter."

And besides, if you have gained control over the victim's command prompt, you can do much worse than just launch a denial of service: Convince the user to type a command that adds their machine to your botnet army, or put that command in the batch file! Why stop at denial of service when you have remote code execution?

Raymond Chen

Follow