It rather involved being on the other side of this airtight hatchway: Denial of service by high CPU usage

devblogs.microsoft.com/oldnewthing/20140529-00

May 29, 2014

Raymond Chen

We received the following security vulnerability report:

> Windows is vulnerable to a denial of service attack that consumes 100% CPU.
>
> 1. Use the following procedure to create a file that is enchanted by magic pixie dust: […]
> 2. Rename the file to `TEST.EXE`.
> 3. Execute as many copies of the program as you have CPU cores.
>
> Observe that CPU usage climbs to 100% and never goes down. This a clear demonstration that Windows is vulnerable to a denial of service attack from magic pixie dust.

The magic pixie dust is a red herring. This vulnerability report is basically saying "If you are allowed to run arbitrary programs, then it is possible to run a program that consumes all the available CPU."

Well, duh.

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. (Or in the lingo of Internet memes, "High CPU is high.")

Now, of course, if the magic pixie dust somehow allows a user to do things like access resources they do not have access to, or to circumvent resource usage quotas, then there would be a serious problem here, and if if the high CPU usage could be triggered remotely, then there is a potential for a denial-of-service attack. But there was nothing of the sort. Here's a much less complicated version of magic pixie dust:

```
int __cdecl main(int, char **) { for (;;) { } /*NOTREACHED*/ }
```

Raymond Chen

Follow