Starting on the other side of this airtight hatchway: Running a program that leaks memory

devblogs.microsoft.com/oldnewthing/20231114-00

November 14, 2023

Raymond Chen

A security vulnerability report came in that said

> In the most recent Windows Insider Build, the `ping` program has a small memory leak. This is normally not a problem because the `ping` program runs for less than a minute before exiting, but if you run `ping -t`, then it will ping the destination machine indefinitely until killed. This can be used as a denial of service if you just start a `ping -t` and let it run. It leaks about a megabyte a day.

While it's true that you could use it as a denial of service, it's also not a very effective one, given that the memory leak is "only" a megabyte a day.

Furthermore, in order for an attacker to exploit this, they need to gain the ability to run programs so they can run `ping -t` and giggle with glee as the program slowly leaks memory.[1]

Since this presupposes that the attacker can run a program with arbitrary command lines, the attacker may as well use something that consumes memory at a far faster pace:

```
for /L %i in (1,1,1000000) do start eventvwr.exe
```

This launches a million copies of Event Viewer, which will certainly mess up the system faster than a one-megabyte-a-day leak.

What we have is a bug but not a security bug. The development team fixed the memory leak, so this bug didn't exist for very long.

[1] In practice, the program will have to leak several gigabytes of memory before the system will start to suffer, so the attacker is in for a wait of several years before their denial-of-service attack finally bears fruit and the system owner will have to either kill the rogue `ping` process or reboot the system. "With this fiendish attack, I can mildly inconvenience somebody a dozen years from now!" (Assuming they leave the system running without rebooting.)