It rather involved being on the other side of this airtight hatchway: Attacking the system clock

devblogs.microsoft.com/oldnewthing/20160107-00

January 7, 2016

Raymond Chen

A security vulnerability report came in that went something like this:

> An attacker can trigger a buffer overflow in the XYZ component by setting the system time beyond the year 9999. This can be used as a precursor step for a further attack.

Thanks for letting us know. We'll look at it.

But is it a security vulnerability?

In order to change the system time, a user must have *Change the system time* permission, which is by default granted only to Administrators and SYSTEM. Therefore, a human being intending to launch such an attack would already need administrator privileges, at which point, they can just stop the XYZ component manually without needing to mess with the system time.

You might think, "Oh, but what if somebody sets up a rogue time server that broadcasts that the current time is January 1, 10000?"

We discussed this a while back. By default, the time service refuses to change the clock by more than 15 hours at a time.[1] That is to prevent exactly this type of attack: Where a rogue time server is messing with the clock in order to trick a computer into setting the time to something that can be used as a foothold for the next level of attack.

Still, this is a good bug to know about. Fortunately, we have around 8000 years to fix it. (But after 7000 years, it'll start getting urgent, so best to set a "Must fix" deadline of around the year 6000, just to be safe.)

[1] The default maximum time skew is 15 hours for workgroup-class machines. There is no default maximum time skew for domain-joined machines. "But wait, doesn't that mean that I can use a rogue time server to manipulate the clocks of domain-joined computers?" No, because domain-joined computers take their time from the domain controller, and those time synchronization packets are digitally signed. If you can forge time synchronization

packages, then that means that you have stolen the private key of the domain controller, at which point, why are you wasting your time with small potatoes like spoofing the system time on workstations?

Raymond Chen

Follow