Protection: Staying up-to-date is staying safe!

|

Rob Tompkins, CISSP, Lead Cybersecurity Engineer, Tulane IT Information Security Team

View PDF

Software. To paraphrase Dickens, it is the best of things, it is the worst of things. It drives all the technology around us but is constantly in need of patching or replacement.

For example, Tulane had been using Trend Micro as its anti-virus (AV) solution for years, but it needed to be replaced. Recently, we partnered with CrowdStrike to use

their advanced endpoint detection and response (EDR) solution. Traditional AV is like a security system monitoring the doors and windows of your house. CrowdStrike EDR is like adding a motion sensor that detects any unwanted movement inside.

When software doesn't need to be replaced, it still needs to be patched. One of the worst data breaches to date is the Equifax Data Breach. The financial records of 143 million people were compromised. There were lawsuits, Senate hearings, and resignations. The worst part: it could have easily been prevented!

Essentially, the Equifax breach was caused by a vulnerability that was patched months before the attack happened. Because the systems did not have that patch installed, it allowed the hackers to gain access to the company's network. How could this happen?

Age is the enemy of technology for both hardware and software. It quietly creeps up on systems, eroding their usefulness. If you aren't paying attention, it will get you. Just a few years ago, in 2019, the US Air Force finally decided to do away with 8-inch floppy disks at their nuclear launch sites! Those disks had been around since the systems were installed in the 1960s.

I am sure that you are not running eight-inch floppies on your machine, but is your system severely out-of-date? Today, the average age of a computer is between three to four years old. Perhaps, you are thinking that is really old, or perhaps you are thinking the jelly donut stain on your keyboard is older than that. There is an unwritten rule in technology circles that five years is the maximum lifespan of a computer. Anything beyond that and you get into some dangerous territory filled with vulnerabilities.

A vulnerability is any software bug that would let an attacker interact with the software in a way that was not intended. It is essential to patch vulnerabilities and upgrade or replace outdated software as soon as possible.

The sad reality is that most attacks involve vulnerabilities that can be patched, but the patch has not been applied. This is like complaining about the rain while holding a closed umbrella.

The Ponemon Institute study Costs and Consequences of Gaps in Vulnerability Response found that 60 percent of breaches were linked to a vulnerability where a patch was available, but not applied. Only 5 percent of the 185,000 vulnerabilities tracked today score a 10.0, but operating systems are prime targets. This image

shows the number of those super critical vulnerabilities by Windows OS.

Today, there are 184,000 tracked vulnerabilities. A minute fraction of those (5 percent) rank at a 10.0. That is the absolute highest score you can get. These super-critical vulnerabilities are the ones that keep security admins up at night.

Propersky.com explains them here:

“Why is [a CVSS 10.0 vulnerability] such a big deal? With barely a few keystrokes, cybercriminals could waltz into some of the world’s largest company’s servers, completely bypassing password, two-factor authentication, and in-server security. Once penetrated, hackers could do anything they’d like.”

Those CVSS 10.0 vulnerabilities show up in everything, and operating systems (OS) are a prime target!

It is not uncommon to find people still running older versions of Windows. The older the OS, the greater the number of super-critical vulnerabilities. As if that is not bad enough, the number of patches produced to fix those bugs goes down as the system ages. Windows 7, for instance, stopped receiving software patches in 2020. If you, or someone you love, is still using Windows 7 or Windows Server 2008, please stop them! It is just not safe anymore.

Updates are essential for every device, whether it’s a laptop, phone, tablet, smartwatch, or other smart gadgets in your home. Windows, MacOS, Linux, Android,

or any software, will have vulnerabilities that need patching. The software update on your phone is about more than just new icons and emojis–it is one of your best defenses against hackers.

Upgrade early, patch often, and stay safe online!