Top

Newsletter 7/27/2022

Back to Contents
A Printable PDF of this post is available here.

The Best Time To Patch Is Always Now

Source: https://wholesaletirescompany.com/wp-content/uploads/2021/08/How-Much-Does-It-Cost-to-Patch-a-Tire.jpg

In Palo Alto Networks, **2022 Attack Surface Management Threat Report**, a statistic was reported that, although well known, up until now had not been well documented. What the networking vendor concluded was that "**attackers typically start scanning for vulnerabilities within 15 minutes of a CVE being announced**," was how Bleeping Computer reported on the summary, July 26, 2022. A CVE is an acronym for **Common Vulnerabilities and Exposures**. The CVE program in the US is associated with Carnegie Mellon University. **The organization defines its mission as follows**:

> **The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program. Partners publish CVE Records to communicate consistent descriptions of vulnerabilities. Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities.**

So a CVE announcement is an universally recognized authority describing, cataloging, and publicizing computer vulnerabilities as these computer vulnerabilities become known. People like me track the CVE announcements daily because I will update my software as soon as there are any newly announced vulnerabilities that may affect my software. I also advise my clients to update their relevant software ASAP. So as much as a CVE announcement is a **SHIELDS UP**! moment for concerned and enlightened computer users and a call to arms to patch now, it is also a statement for the hackers to arm their **Photonic Cannons**. The CVEs tells the hackers where to point their cannons — to extend the Star Trek/CISA analogy.

That the hackers use the CVE system as road maps to new forms of attacks has been a known weakness of the CVE concept from its inception. The essential problem is one of timing and the needed depth of knowledge required to launch an attack compared to all the resources needed to fend off an attack. **Security vendor, UpGuard, described the imbalance, and how the CVE systems helps counter the imbalance**:

> **Organizations need to protect themselves and their networks by fixing all potential vulnerabilities and exposures while an attacker only needs to find a single vulnerability and exploit it to gain unauthorized access. This is why a list of known vulnerabilities is so valuable and an important part of network security.**

Let's take a look at a recent CVE announcement. **July 13, 2022, BleepingComputer**, reported that "**Lenovo has issued a security advisory disclosing three medium severity vulnerabilities tracked as CVE-2022-1890, CVE-2022-1891, and CVE-2022-1892**." To its credit, **along with its announcement of the vulnerability, Lenovo issued a firmware update to correct the problems**. Since this vulnerability is limited to certain Lenovo motherboards, users who rely strictly on Windows monthly updates to patch their systems, might not get this update applied. The user would have to be aware of the need to patch. Another obstacle to patching UEFI vulnerabilities is many users are just not going to apply motherboard and other firmware patches since such updating does require a certain amount of technical know-how. So while many users will not scroll the Lenovo announcement and find their model to know to what patches to apply, it is now known and certain that hackers have already done so and planned their attacks accordingly.

An attack on the UEFI firmware can be the most destructive, and yet the most difficult to detect and mitigate against, because the attack takes place before the operating system loads. Even replacing the hard drive will not cure the computer infection. So what does an owner of an older ASUS computer or a DYI computer with a GigaByte motherboard do, when as **BleepingComputer reported, July 25, 2022**, an UEFI vulnerability has been detected by antimalware vendor, Kaspersky Labs, in older motherboards by these manufacturers? These attacks are believed to have been ongoing since 2016. No motherboard patches have been issued. And since these are all discontinued models, it is unlikely any such mitigations will ever be offered.

At the core of the issue is best summarized by the ArsTechnica headline about the ASUS/GigaByte situation. "**Discovery of new UEFI rootkit exposes an ugly truth: The attacks are invisible to us**." The same article states clearly the appaling truth of UEFI attacks. "**Turns out they're not all that rare. We just don't know how to find them**." Hard to find because the attack doesn't live on a hard drive. And that is what antimalware software scans for.

The main push of this article is that there may only be 15 minutes from a CVE announcement to the possible exploitation of that newly announced vulnerability. There is just no rationale for not applying patches as soon as you are aware of them. Run Windows Update frequently, if not daily. Do the same with Google Chrome. If you are not sure how, check out the **cheatsheets**.

If that older PC is starting to slow to a crawl there is a high likelihood that a UEFI rootkit is reinfecting the PC every time the machine starts. Moreover, there may be no fix for the problems no matter what.

In the 60s, a common counter culture saying went like this: "**Either you are part of the solution; or you are part of the problem**." I say: Don't complain about having to patch. Be glad that you can. Because, as a wise man once said, "**There is no magic wand that can resolve our problems. The solution rests with our work and discipline**."

"The devil did not need to work at all when people were so willing to do his dirty work for him."

— E.A. Bucchianeri, Vocation of a Gadfly

Back to Top

Gerald Reiff

Back to Top **next post →**