February 2024

As we wrap up the second month of 2024, let's take a look at a few of the notable publications and work to gain an understanding of everything that has happened. Although the theme of these can seem to be familiar, with patching being a big mitigation to many threats, it is worth noting that the only way that you can know when something needs to be patched is to know the systems that you work with. Although it is easy to point the finger at the vendors and providers, you have no way to keep up if you don't know your software and systems. It is also worth mentioning that while OSINT is a great avenue of information, that information is only valuable when you take action on it.

Starting with the more notable vulnerabilities, ranging from 3D printers to WordPress. The AnyCube vulnerability found in the 3D printers of this company is gaining traction as user post that their machine has been making waves in forums after the person behind this attack vector started pushing a .gcode file to the affected machines. This file type is normally where the print files are sent for normal printing instructions. The good news is that this is not a malicious file and just displays a message warning users that their machine is vulnerable, and they should disconnect it from the internet until the company patches the flaw. This is a good example of someone leveraging a vulnerability to warn users in the hopes of pushing the company into fixing the issue. Switching gears to the heavily targeted business email systems, ShadowServer annonces that over 97K exchange servers remain vulnerable to CVE-2024-21410 as of February 17th. The scan run does not take into account if administrators have applied the mitigation steps, this is still a staggering number of potential vulnerabilities. The scope of this spans the globe with most major countries with 10s of thousands of vulnerable servers.

With a staggering 5 vulnerabilities, all ranking in at a CVSS score of 8 or higher, SolarWinds pushes out patches to the ARM and Access Rights Manager that where vulnerable to path traversal attacks. As of the writing of this, there have not been any disclosed exploits in the wild for these. This is a good highlight to take away that attackers focusing on the supply chain can have unmeasurable impact as the surface of the attack has a far-reaching ability. Another example of a supply chain related threat is the disclosed vulnerability in the WordPress LiteSpeed plugin. Putting 5 Million sites at risk of a SQLi injection, the tactic can allow attackers to gain information on the stored data. Not only does this allow attackers to gain knowledge an intelligence of the users, depending on what is stored in the database, this can also reveal sensitive information like PII or login information. Although the CVSS is only at a 6.4, it is worth noting that any type of attack may not be as harmful with the specific attack type but can lead to more detrimental consequences when chaining with multiple attack types.

Taking a look back at the Microsoft Patch Tuesday for February, the software vendor has released patches for 73 flaws. Within these, it does include fixes for two Zero-Days that have been actively exploited in the wild. Hardening and security products are fantastic and while you can have the most robust stack, you will never be able to protect against tank. With flaws ranging from elevation of privileges to spoofing vulnerabilities, just remember that as the IT and Security professionals, we have to get it right 100% of the time while the attackers just need to get lucky once. Keep this in mind as you work to get better within the industry. We are the ones that others rely on for their safety.

Jumping into the unknown, let's take a quick look at a couple tips for keeping safe with AI. In the new frontier it is inevitable that users will want to leverage the new technology to help improve the quality and productivity. Learning how to keep the usage of this safe is going to be of paramount importance. Like many software and systems before it, the best tips are just reiteration of everything before it. Of course, rotating the secret or password used can only help to keep the account itself safe. Next, making sure to clean up any data BEFORE processing it into the LLM will help to ensure that you do not unintentionally feed information that the LLM can use for other requests. Remember that unlike a google search, the LLM will use the information input to help not only you but ANYONE else that queries the engine.

Finally, knowing what the attackers are doing is another tool in the arsenal against them. Unfortunately, Google's TAG has announced that 80% of the zero-days discovered in 2023 were created by commercial spyware vendors. Although they may have created them with the intent to help, these are often used by threat actors. Showing us that not every threat actor is the wolf hiding in the dark. Sometimes they can be wearing the sheep costume and blending in with the rest of the herd. Although the vulnerability was patched, the disclosure that the threat group known as Lazarus is behind the 7.8 CVSS Kernal level flaw in Windows OS. The cat and mouse game that is the world of technology is ever present. Knowing the number of resources at their disposal only exemplifies the fact that these are organizations. With R&D just like a legitimate company, they are constantly finding new ways to get in or profit from the illicit means.

As we look through the events of the month, lets start thinking about what is next. Although it is extremely important to know your technology stack and what needs to be patched an when, is it time to start looking to a full solution? Is Zero Trust the answer to this? Personally, I hope so. Learning and making sure to stay informed is going to be the only way to make sure that you are not falling behind.