Caleb Leggett

January 15-26

As we have missed a week, let's take a look back through the last two weeks in Cyber Security. As you may well know, breaches can happen from many different vectors and attackers are always looking for that next way in. Whether that is through the server that contains the data, the hardware that powers the devices or the applications used, flaws are constantly found, patched and then pivoted in the ever-going cat and mouse game between the threat actors and the companies creating the software and hardware. As always, this is not meant to be an all encompassing review but just a glimpse into the world of Cyber.

In the hardware side, let's start with the GPU leak found in AMD, Apple and Qualcomm where AI data is leaked allowing for a LeftoverLocals attack. Discovered by Trail of Bits researcher Tyler Sorensen, the attack allows for threat actors to extract data from LLM computing by simply adding a listener to the GPU. This can result in the attacker gaining access to sensitive information that was input by the user into the LLM. While apple and Qualcomm have released patches to fix some of their chips, AMD and some of the other chips from both other vendors remain vulnerable.

Moving to the server side hosting the data, let's look at two notable releases affecting GitLab and WordPress. The release from ShadowServer shows that over 5,000 GitLab instances are still exposed even after the release of the patches to fix the flaw.

Although MFA can stop this, it is notable that any account without this feature can be vulnerable. GitLab has released steps to check if the environment has been compromised and while there are no reported instances of a successful attack, this should not be meant to postpone actions to mitigate the risk. Next, lets look at the WordPress database plugin attack vector. Unlike the GitLab attack, this is actively being used in an attack vector. The plugin is active on 1 Million sites and is used by admins to find and replace items. Attackers are able to leverage this in a PHP object injection attack. While WP Engine has released version 1.4.5 to address this, it is worth noting that this is a critical severity flaw and should be mitigated as soon as possible. To add to this, Threat actors have created the Balada Injector Malware to leverage this flaw.

Finally, lets look at the software. On Tuesday January 16th, Google releases fixes to the chrome browser to address actively exploited Zero-Day flaws. The flaw targets the V8 JavaScript and WebAssembly engine which can be used to trigger a crash. With this, it then allows attackers access to out-of-bounds memory which can contain a treasure trove of information for the attacker including bypasses for protection mechanisms.

As we move to wrap up this look back, it is also worth noting the discovery of the APT threat targeting HP. Russin backed attackers known as Cozy Bear, have been able to breach the cloud-based email environment. While the threat of a nation state is not always straight forward, knowing the sectors and industries that they target and identifying the reasons behind there attacks is paramount as these can lead to the release of exploits used by other groups that may not be as well funded.

Knowing what systems that you have in the environment and ensuring that you keep up with releases to patches or mitigation can help to identify risks and perform the first steps to ensure that

you are protected. While you may have the best security in place and account for many attack vectors, Zero-Days can be thought of as the burglar using a tank to get in. You may have accounted for any other possibility, accounting for tank is near impossible and this is why staying as informed as possible is the first steps in the world of Cyber.