ROBO6K

512-379-2272
cleggett@robo.net

8/11/2023

It's time again for our look-back in this week of Cyber security. While this is not a complete list of everything going on, it will help to give you an inside look into the need to stay up to date with the world of Cyber. There are many focuses but the two main ones to keep an eye out for are the every evolving world of Spam and phishing and the need to ensure devices stay up to date with patches and updates. While many people using technology will push back on change, patches and updates will be incredibly valuable to help prevent attacks or intrusions.

This week brings about Microsoft's Patch Tuesday and with that the warning of 2 zero-day vulnerabilities as well as 87 software flaws. This helps us bring to mind that no matter how secure you may think your software is, the threat landscape is forever changing and what is secure today, may not be tomorrow. With flaws ranging for escalation of privilege to DoS attack flaws, you will want to ensure that all devices have updated. Keep in mind that the patches talked about do not include twelve vulnerabilities affecting MS Edge. Other things to note from this week are the MS VSCode extension that allows attackers to steal passwords. The threat vector allows Threat actors to steal authentication tokens from MS, Linux and macOS third-party APIs. While this is released as a PoC, Cycode has made a statement that this was reported two months ago but Microsoft engineers have not released any patches or given it the proper concern that it should receive.

Adobe released 20 security patches for the reader program this week. This is a friendly reminder that while ensuring that the OS is updated and patches applied, third party software can become just as vulnerable. With patches to address things like memory leaks or even as severe as security feature bypasses, knowing the entire attack surface of the company will only increase the odds that you are able to maintain that elusive good security posture.

While spam and Phishing attacks have many shapes and forms, there is not many ways to truly combat these things. It is reported that 1 in 3 executive level employees will fall victim to an attack at some point. This is why it is important that no matter your level in a company, spending the extra few seconds to verify the source of emails coming to you is legitimate. While senders or domains can be blocked, that will generally only happen when the attack is caught. Just remember that you as the employee must catch an attempt every time, the attacker only needs to be successful one time.

Attack vectors don't always come from the software side. It has been a tough week for hardware major hardware vendors, Dell, Intel and AMD as major security flaws have been discovered. With Dell Compellent Integration Tools the risk of leaked admin creds for the VMware integration can become discovered. Pointing out that the security of the backend appliances are just as integral as the end user devices. Researchers have discovered that a feature of every modern processor allows attackers to use the Dynamic Voltage and Frequency feature to deduce changes in the CPU. With the proper understanding of how this works, attackers can then leverage power side-channel attacks which can be done remotely. Dubbing the attack HertzBleed, intel and AMD have both written this attack vector off stating that the knowledge and expertise needed are to reproduce this attack outside of a lab environment.

On a good note, Google has announced a change in their update schedule from bi-weekly to weekly in an attempt to combat attackers from exploiting the application. Keeping your browser updated is an important step to take to ensure that you are safe while perusing the internet safely. The change will start with Google Chrom 116 so keep your eyes pealed as this is an extremely easy thing for helping your internet presence continues to stay as safe as possible.

As always, stay vigilant and remember, only you can ensure that your experience online, whether for work or your personal life, relies on YOU. If you have any questions regarding any of the information found here, please do not hesitate to reach out to the security expert or colleague.

Thank you,

Caleb Leggett

Your ROBO Technician