

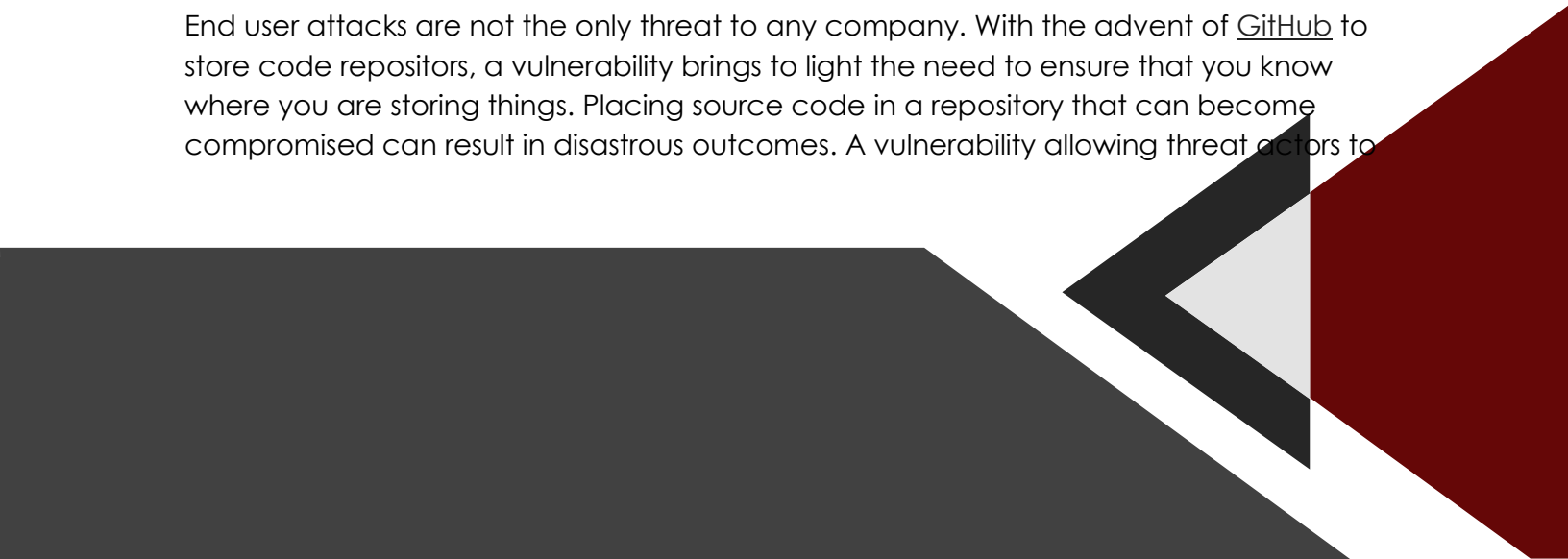
9/11-15

As we look back at this week in Cyber, the need for continues to be at the forefront of combatting issues. With Septembers Patch Tuesday, Apple Zero-Day patches as well as a few others, this is a stark reminder that no matter how good of a security posture that you may have today, that can and will change tomorrow.

Although this month saw a smaller number of patches from [Microsoft](#), with only 2 zero days and 59 flaws being patched, keeping up with these is of paramount importance to ensuring that any other cyber security measures taken will continue to remain affective. Microsoft was able to patch vulnerabilities in categories ranging from security feature bypass to spoofing vulnerabilities. Unfortunately, the two zero-day exploits were being actively leveraged in the wild with one local privilege escalation tactic and one information disclosure technique.

Microsoft is not alone in their release of patches this week with companies ranging from software to virtualization releasing patches of their own. This begs the question; do you keep all of your personal equipment up to date? Both [Google](#) and [Apple](#) release patches for actively exploited attack vectors.

End user attacks are not the only threat to any company. With the advent of [GitHub](#) to store code repositories, a vulnerability brings to light the need to ensure that you know where you are storing things. Placing source code in a repository that can become compromised can result in disastrous outcomes. A vulnerability allowing threat actors to





perform what is called Repojecting, at least 400 code packages have been stolen using the discovered vulnerability.

Although these are not the only patches, the hope is to continuously remind you that it is extremely important to not only make sure our client systems are up to date, but even your personal equipment. Remember, attackers find victims of opportunity and will go after anyone that they can, be that a business or a single user.

Let's also take a moment to look at the attack on the [MGM resorts](#). While this is not the first attack, it goes to show that the more that a company relies on technology to perform their specific function, the more detrimental that it can be. The attack is expected to be a ransomware attack stemming from a Vishing attack. In the initial investigation, the attack comes across as extremely easy to accomplish as the attackers most likely visited the company LinkedIn to find the name of an end user and then contacted the help desk to launch the attack. This is not the only casino that has been hit recently as [Ceasars](#) was also hit with their disclosure coming any day now. Ceasars resort mitigated the attack by paying a small \$15 Million to the attackers. Keep this in mind that it is extremely important to know who you are talking to when servicing requests and that if a request to reset someone else's password comes through that you know a few things before doing this. Things like who is requesting this? Should I provide the new password or work with the end user after the initial request?

As always, stay vigilant and always remember that you are the first line in the defense of not only our clients but of your personal life as well.

Caleb Leggett



