October 9-13

As we take a look into this week we will focus on zero-days and patches as our focus. While Zero-Day threats are very scary as they are the first discovery of an attack vector, it can be just as important to maintain the patching on your systems. While both subjects tend to come up a lot, there is a good reason behind that. IT IS VERY IMPORTANT. First in understanding the need to keep up with everything going on within the world of cyber security and knowing what software and hardware you are using to know when new attacks are discovered but also to make sure that you are applying the patches not only to the systems in the production environment but also looking into the need to apply those patches to any backups that could be pushed back out into production.

Microsoft is at it again with Patch Tuesday for the month. Releasing 104 flaw fixes and 3 Zero-Day fixes, it is important to remember that this is only one company. With flaws ranging from escalation of privileges to denial-of-service vulnerabilities, keeping any software that is in use up to date is extremely important. While an internal assessment gave only 12 of the flaws a critical rating, taking care of the software security is only a piece of the defense in depth model.

While Microsoft is not the victim in the next Zero-day, they where able to release findings of state-sponsored threat group 'Storm-0062' use of a privilege escalation in Atlassian's Confluence Data Center. The attack is believed to have been happening since September 14, 2023, with the attackers having at least 3 weeks to create arbitrary admin accounts and gain access to sensitive data. A PoC has been released by Rapid7 show how the exploit could have been leveraged.

Finally, let's take a look the two major DDoS attack vectors that have come up this week. The first uses the Mirai botnet has added payloads to target another 13 routers using the Linux-based platforms. Suspected threat group IZ1H9 will then use the infected devices in targeted DDoS attacks. The next new DDoS threat is an actual attack type,

becoming known as a Rapid Reset attack. Attackers can leverage smaller botnets to create a larger impact. With a small 20,000 bot army, millions of requests can be made within a short period of time. By using a request and then cancel in rapid succession, the smaller botnets are able to overwhelm networking appliances and webservers. The attack is yet another Zero-Day for the year and suspected of being leveraged since August. While a few cloud companies have patched the flaw, it was able to break records with Google reporting an attack reaching 398 million Requests per second!!!

Knowing all of this, we just want to reinforce the need to always keep learning. While you cannot be expected to know everything and know every vulnerability, it takes a village to ensure that each house is protected.