October 2-6

It's that time of the week yet again. While many of us may think of a vulnerability as those affecting software or operating systems, this week has shown us that even the underlying hardware can become vulnerable. While these types of exploits are not as common, they can be even more detrimental as they can give attackers access to the highest level of access, the hardware itself. With two different hardware flaws affecting Android devices and one affecting the Cisco security devices. We will also take a quick look at the Zero-day affecting the widely used Apple devices.

An exploit targeting the widely used ARM GPU used in many android devices was found by the Google Threat Analysis Group(TAG) was released. While an updated driver can close the attack vector, the need for patching cellular devices is brought to mind with this exploit. The exploit allows an attacker with 'local non-privileged access to make improper calls to the memory processing operations to gain access to already freed memory' ARM explains. There has not been much more information regarding this exploit that has been made publicly at this time.

As often is, multiple attacks can become known for similar operating systems at the same time. Qualcomm, another cellular chipset maker, has released three CVEs. The flaw, discovered by Google TAG, is rated with a high severity. Unfortunately, there is not much past applying the patched drivers currently. With the ARM release, there has not been much more information regarding this attack vector.

While we pivot to another exploit, Apple has released patches to address an actively exploited Zero-Day flaw. While the attackers and nature of the attack are currently unknown, the only upside is that the attacker would already need a foothold in the device in order to exploit this attack vector. With this new development, that brings the total to 17 actively exploited iOS Zero-Day flaws so far this year. While many think that just because you use an apple device, that you are secure, always keep this in mind, no matter the device or operating system, attackers will wind a way in.

Another point to note about the MacOS, while historically Apple has been considered a more secure OS, threat actors have been looking to change this. Ads within the darknet community are offering up to $1 Million for an exploit for the system. With offers this high, it is inevitable that someone will find a way into the system. This is important because as many Mac users are set up with local administrator privileges.

The importance of looking into the entire environment is extremely important. While you may not know all of the underlying hardware in every device, it is important to keep your eyes and ears open. Remember that you as the technical person are responsible for ensuring that you protect the end user to the best of your ability.

Your Name