Caleb Leggett

10.30-11.3

As we wrap up another week, it is time again to look into the world of Cyber Security. While not every exploit is directed at the systems that you use, it is important to remember to keep up with those since the target of the attackers can change from day to day. While many of the ‘hacktivists’ are focused on the battle at hand, those battles and wars will eventually come to an end. Being aware of the tactics that they are using today can help secure you for the future. We will also look at the PoC for the security vulnerability of the security system. We will wrap up with a look into the new CVSS severity rating system.

Groups like North Koreas Lazarus group or Iran’s Scarred Manticore bring to light the need to keep up with the tactics that are being used in active conflicts. While the threat actors may not be targeting systems used by you today, the focus of the attackers can change, or the exploits used can be resold in the C2C market, so it is worth noting that keeping up with these attack vectors is very important. By leveraging the virtually limitless resources that being backed by a nation-state gives the organizations, they can take on larger targets and accomplish things that a smaller group is able to.

Realizing everything in your network that is connected can help you to realize the true attack surface. With the PoC targeting Wyze cameras, it brings to light the need to realize the full scope of the attack surface. The exploit allows attackers to perform RCE in the Linux shell which would give them the ability to pivot into other systems on the network. The release of the PoC does come with a little controversy as the researcher that found the vulnerability released this before the company had time to patch the systems. Although they have been patched at this time, knowing when things are released can help shed light on if you should be aware of the vulnerabilities.

While standards may not change often, it is important to remember that they do in fact change as many things in the technological world do. The forum of Incident Response and Security Teams (FIRST) officially releases such a change to the way that vulnerabilities are rated. The biggest thing to note on these changes it the granularity that it now offers security teams. By adding this granularity, it strives to improve assessment of releases and gives an understanding of the priority to which they should be addressed. The other advantage that the new ranking system gives is the addition of IoT/ICS/OT systems into the fold. This allows teams to identify risks and act in the correct priority and to all for better risk management.

As we wrap up this week, it is important to remember the takeaways. Whether you are being directly targeted or not, knowing what is going on in the world of cyber and the threat vectors being used can allow for better protection of data and systems. As discussed, the need to know your full threat landscape and all systems within the network can make the difference between protecting the entire network and allowing for an attacker to gain a foothold into the systems. Finally, keeping up with the industry standards and changes can keep you in the know. While this is not everything happening in the world of cyber security, remember that keeping as up to date as possible lies in the hands of you as the technical specialist.