APPLYING LESSONS FROM CISA TO YOUR FIRMWARE

The Cybersecurity and Infrastructure Security Agency (CISA) recently published alert AA20-245A, *Technical Approaches to Uncovering and Remediating Malicious Activity*. The alert serves as a playbook for security incident investigations based on the collective real-world findings of security agencies from Australia, Canada, New Zealand, the United Kingdom, and the United States.

The alert defines key steps and techniques for the detection, response, and remediation of security incidents. The guidance also calls out some of the most common mistakes made during the incident response process and stresses the importance of ensuring that forensic data is preserved and that threats are thoroughly eradicated to prevent a recurrence of the problem. The recommendations cover these topics from multiple security disciplines including host-based security, network security, as well as recommendations specific to network infrastructure among others.

Firmware security plays a critical role in a variety of the best practices set forth in the alert. In some cases the alert specifically cites firmware, and in others, firmware is a part of a larger security discipline. To this end, let's take a closer look at AA20-245A through the prism of firmware and hardware security.

APPLYING THREAT DETECTION STRATEGIES TO YOUR FIRMWARE AND HARDWARE

CISA calls out several approaches to threat detection which are broadly applicable both from a network as well as a host-based perspective. This includes security basics such as searching for Indicators of Compromise (IoCs) tied to known threats as well as more behavioral approaches to detection based on pattern and frequency analysis to identify anomalies.

Security and IR teams should keep in mind that these topics are particularly important in the context of firmware. The firmware layer of devices provides attackers with a variety of places to hide and maintain persistence. Here are a few points to keep in mind when applying detection strategies to firmware.

- **Don't Let Attackers Hide in Code Caves** - IoCs are great, but only if security can actually see them. Attackers have realized that they can hide their malicious code and assets in firmware as a way to avoid inspection by AV and EDR tools. Even a few unused bytes in firmware code caves can allow attackers to hide things like encryption keys without being seen.

- Check for Firmware Rootkits, Implants, and Backdoors - Firmware rootkits and other hardware implants are invaluable to attackers as they can give an attacker complete control over a device and its operating system. Teams should verify the integrity of the firmware on their devices including system firmware such as BIOS/UEFI as well as firmware within device components. Tools such as CHIPSEC or Eclypsium can make it easy to make sure firmware matches known good versions of vendor-supplied firmware as well as to detect known firmware implants.

- Firmware Behavior Should be Very Predictable - Firmware also provides one of the more reliable places to perform behavioral analysis to detect unknown threats. This is because the behavior of firmware tends to be very predictable when compared to higher level software and applications. This makes it far easier to tightly baseline normal behavior and recognize deviations that would indicate a threat.

DON'T FORGET ABOUT YOUR FIRMWARE AND HARDWARE VULNERABILITIES

When discussing vulnerabilities, the alert notes that "Attackers frequently exploit software or hardware vulnerabilities to gain access to a targeted system" and that "vulnerabilities in external facing devices and servers should be patched immediately." This highlights the critical role that hardware and device-level vulnerabilities play in an organization's overall security. Organizations need to be able to address all relevant vulnerabilities within an externally facing device regardless of whether the vulnerability resides in software, firmware, or hardware. Attackers are naturally free to exploit any vulnerabilities that are exposed and are not limited to only attacking software. As threats have increasingly targeted hardware and firmware, it is up to organizations to make sure that weaknesses in these areas are identified and patched.

- **Add Firmware to Your Vulnerability Management Program** - While most organizations spend considerable effort to find and patch vulnerabilities, traditional scanners are typically blind to vulnerabilities within firmware. This is a major gap as vulnerabilities at this layer are common and potentially devastating to the security of a device. Vulnerabilities such as the recently discovered BootHole vulnerability apply to the majority of Linux and Windows based systems and can allow an attacker to take full control of a device and its operating system even when Secure Boot is enabled. Teams need to be able to scan for critical firmware vulnerabilities and misconfigurations not only to ensure that devices can be reinfected, but also to remove hiding spots that attackers use to maintain persistence.

FIX IT RIGHT THE FIRST TIME TO AVOID SECURITY WHACK-A-MOLE

CISA's alert also calls out some of the mistakes that teams often make when responding to a security incident. This included a tendency to address the symptoms of an attack without thoroughly getting to the root cause of the threat. The alert specifically urges teams to "ensure the actor is eradicated from the network" and to "avoid residual issues that could result in follow-up compromises once the incident is closed."

Firmware plays a critical yet often overlooked role in this area as well. Without the ability to root out threats at the most fundamental layer of a device, security teams can easily find themselves in an IR loop without ever getting to the root cause of the problem. Teams should consider building the following steps into their security and IR practice.

- **Add Firmware Integrity Checks to Your Device Recovery Program** - Re-imaging a device is a standard practice for devices that have been infected with malware or otherwise potentially compromised in an attack. However malware has taken to hiding within firmware as a way to persist across a full reinstallation of the operating system. Even small amounts of code can allow the attacker to regain control over the system once it is returned to use. Teams can easily and automatically look for these types of threats by performing integrity scans of all device firmware before it is put back into service.

REMEMBER THAT NETWORK INFRASTRUCTURE IS PART OF THE ATTACK SURFACE

CISA naturally calls out a variety of network security best practices to help organizations to defend themselves. However, the alert also focuses on the need to secure the networking infrastructure itself. Vulnerabilities in network devices have become some of the top targets for all types of attackers, security teams need to ensure visibility into these systems for weaknesses and signs of compromise. Given the tight coupling of firmware and operating systems in networking devices, security teams will naturally need to keep an eye on all the code running in these critical devices.

- **Keep Network Devices Up to Date** - A series of recent vulnerabilities such as those found in Palo Alto Networks PAN-OS and Cisco's IOS have made network and security infrastructure highly visible targets for attackers. The CISA alert specifically calls out the importance of keeping router firmware up to date and ensuring that all networking devices including switches, routers, and firewalls use secure images. As a result, organizations should ensure that all systems are patched and updated, and teams should additionally verify that the firmware on network devices is current and free from significant vulnerabilities. The availability of automated tools ensures that scans can be done easily and performed at regular intervals instead of waiting for the inevitable emergency.
- **VPNs Are in the Crosshairs** - VPN infrastructure has become an even greater priority as organizations increasingly seek to support secure remote work for employees. These same security components have likewise become some of the most common targets for attackers. The CISA alert calls out the importance of ensuring that VPN infrastructure is kept in a secure state and free from unnecessary exposures. Auditing the firmware of these devices is a key part of maintaining the health of these all important components. To keep pace with the rate of new vulnerabilities, organizations may want to consider automated scanning tools to ensure the firmware VPNs and other network devices are up to date and free from weaknesses.

CONCLUSIONS

CISA's AA20-245A covers a great deal of security territory and best practices. The key takeaways of the document are structured to make sure that organizations can find threats, capture the information that they need for analysis, and conclusively remediate incidents. While firmware is not the focus of the alert, firmware does play an important role in many of the techniques and principles that are covered. Using tools such as the CHIPSEC framework and the Eclypsium platform, organizations can start to consistently build firmware and hardware security into their best practices. If you would like to learn more about how Eclypsium can help your organization, please contact the Eclypsium team at info@eclypsium.com.