ASSESSING FIRMWARE SECURITY RISK IN 2020

5 questions to evaluate and improve your firmware security posture

INTRODUCTION

2019 had the most firmware vulnerabilities ever discovered, marking a 43% rise over the previous record in 2018, and a staggering growth of 750% since 2016. In many ways it was a transformative year in which firmware security hit the mainstream. Leading analysts sounded the alarm on the immediate need for better firmware security for enterprise devices and the risk to organizations that fail to adapt. Firmware gained increased focus for regulatory compliance as standards continued to map to the NIST Cybersecurity Framework and its detailed focus on risks and threats at the firmware layer. Manufacturers further validated the growing risk by stepping up their efforts to address firmware and hardware security at the platform level.

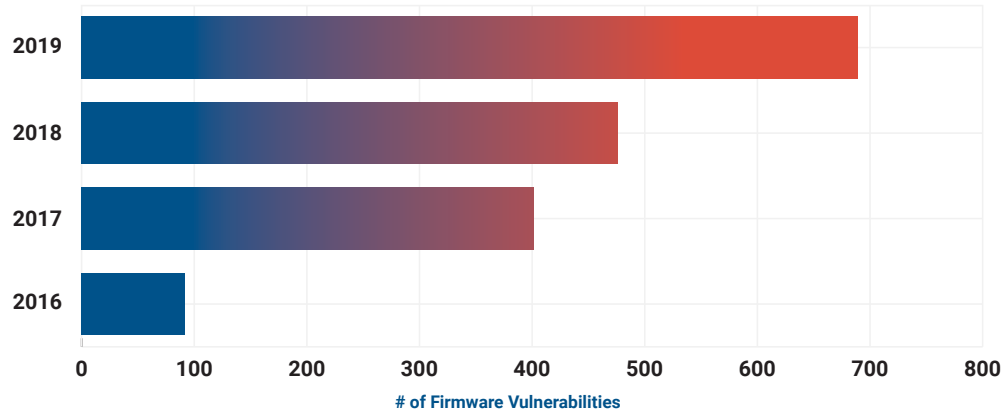
In addition to the ongoing surge in vulnerabilities, attacks in the wild continued to target firmware in order to achieve persistence, evade security controls, and further strategic attacks. F-Secure found that compromised firmware was the 3rd most common infection vector in 1H 2019, accounting for 12% of attacks disrupting companies, public entities and other organizations. Attacks followed a variety of paths including the well-worn progression of malware attacks, network-based attacks, as well as hardware and supply chain attacks.

With these developments in mind, this report aims to give security teams and their leaders a way to self-assess their firmware security in light of the biggest trends of the past year. In each section we pose a fundamental question concerning firmware security readiness and why it is important based on the events of the previous year. While not an exhaustive list of firmware security topics, we hope that these questions can give organizations a way to begin evaluating their risk with regard to firmware.

1 Do You Have Visibility Into Your Firmware Vulnerabilities & Assets?

Vulnerability management is unquestionably one of the most fundamental aspects of a solid security program. And while vulnerability scanning and patching efforts are standard practice for software and operating systems, most organizations lack that same rigor for the firmware in their devices. These lapses have become a serious liability in 2019 both in terms of potential risk and realized threats.

First, the discovery of new firmware vulnerabilities has continued to skyrocket. 2019 was the third consecutive year to set a new record for firmware vulnerabilities, growing 43% over 2018. The total number of CVEs was 7.5 times larger than what was documented just three years ago. Firmware vulnerabilities can also be found in virtually any component within a device including the system firmware such as UEFI or BIOS as well as drives, network adapters, memory, processors, graphics cards, and so on.



Source: National Vulnerability Database December 31, 2019

Weaknesses in firmware can be particularly high impact vulnerabilities due to the privileges and control they can provide to attackers. The combination of privileges with stealth translates to real-world impact, which can be seen in the MITRE ATT&CK framework where firmware is featured prominently in the categories of Defense Evasion (T1109), Persistence (T1019, T1109) and Impact (T1495).

In addition to vulnerabilities, organizations must have visibility into the reliability of their assets. Devices should be running up-to-date and supported firmware in order to ensure their best performance. However, most organizations lack the basic visibility to know if the firmware in a device is current or even supported at all in the case of legacy devices.

As you consider the organizational risk of firmware and its impact on your asset and vulnerability management programs, we encourage you to review some of the recent Eclypsium research. These provide examples of real-world, exploitable vulnerabilities that you can use to help assess your visibility and management. The table below summarizes some of the most notable vulnerabilities found by Eclypsium in the past year.

Topic	Summary	Further Reading
Driver Vulnerabilities	Discovery of widespread issues affecting more than dozens of drivers across 17 different vendors. These powerful drivers can be used by attackers and malware to escalate privileges and potentially add firmware implants that can subvert the boot process and the OS itself.	Screwed Drivers The Mother of All Drivers
Remote Server Vulnerabilities	Vulnerabilities in baseboard management controllers (BMCs) of servers, which allow an attacker to easily connect to a server and virtually mount any USB device of their choosing to the server, **remotely** over any network including the Internet.	USB Anywhere
Vulnerabilities in the Supply Chain	Discovery of vulnerabilities in a 3rd party firmware vendor, and how those vulnerabilities ended up affecting multiple enterprise-class servers.	Vulnerabilities in the Firmware Supply Chain
Vulnerabilities in Cloud Hosting	Discovery of vulnerabilities in the hardware underlying bare metal hosting services. This style of vulnerability can allow an attacker to install a firmware implant that persists from one customer to the next.	Bare Metal Cloud Vulnerabilities

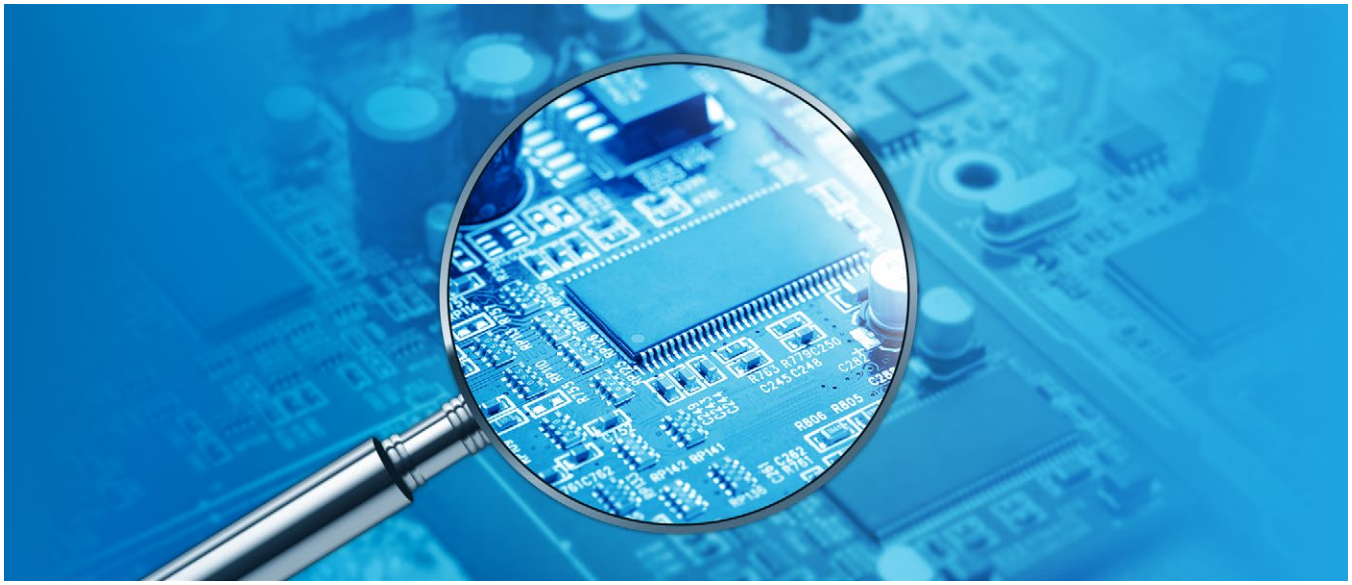
Unfortunately, the firmware blindspot is translating into real impact for organizations. A study by Forrester found that "63% of companies have experienced a data compromise or breach within the past 12 months due to an exploited vulnerability in hardware- or silicon-level security". The impacts of these compromises even extended into critical infrastructure when attackers used simple scripts to attack unpatched Cisco devices, resulting in a denial-of-service against the US power grid. Looking forward, Gartner published a prediction that by 2022, 70% of enterprises without a firmware upgrade plan will be breached due to a firmware vulnerability. The clear consensus is that organizations that ignore firmware vulnerabilities will face an increasingly tough present and future.

> "By 2020, 70% of organizations that do not have a firmware upgrade plan in place will be breached due to a firmware vulnerability"
>
> **—Gartner**

☆ RECOMMENDATIONS

- Gain greater visibility into your potential attack surface by adding firmware attributes to the data collected as part of your asset management program.
- Integrate managing firmware with existing hardware and operating system lifecycle programs.
- In addition to system firmware, ensure you have visibility into firmware vulnerabilities in device components.
- Add regular automated vulnerability scanning for firmware vulnerabilities and misconfigurations.
- Incorporate firmware vulnerability metrics into your existing vulnerability management program reports.
- Conduct an assessment of the discoverability of vulnerabilities in external facing assets using tools such as Shodan and Nmap to understand what adversaries may uncover as part of initial reconnaissance activities.
- Consider tools to streamline the firmware update process.

2 Can Your Organization Detect Firmware Tampering?



Once organizations have visibility into their attack surface, they need to be able to detect the signs of attack. This can include continuous monitoring to detect any tampering of firmware as well as on-demand interrogations in response to suspicious activity. Unfortunately, this is often a challenge when it comes to firmware and hardware. Traditional security controls are often limited to the OS and software layers, and lack visibility into threats at lower levels.

Defense evasion is one of the major motivating factors that drives attackers to the firmware layer in the first place. The ability to hide at the firmware layer provides attackers with some of the most reliable persistence possible, with the ability to persist across full system re-imaging or even replacement of storage drives. Likewise, malicious code within firmware can give attackers the highest levels of privilege, disrupt the boot process of the device, patch the OS itself, and gain near-omnipotent control over the device.

2019 provided ample examples of such threats in the wild:

QSnatch Malware: A new strain of malware was discovered targeting network attached storage (NAS) devices made by technology vendor, QNAP. The malware modified the firmware of victim devices to achieve a variety of ends including stealing usernames and passwords, preventing the update of firmware, and controlling regularly scheduled jobs and scripts.Cr1ptT0r ransomware also infected NAS devices from D-Link in 2019.

JungleSec Ransomware: JungleSec attacked devices over the network by targeting the IPMI interfaces used for the out-of-band management of enterprise servers. Vulnerabilities in IPMI and baseboard management controllers (BMCs) are quite common, and compromises can allow attackers to steal data or disable the affected server entirely.

DoS Attacks Against U.S. Power Plants: Network outages in U.S. power plants were attributed to firmware vulnerabilities in Cisco ASA firewalls. NERC provided a detailed 'Lesson Learned' analysis entitled Risks Posed by Firewall Firmware Vulnerabilities. This attack also underscores the importance of including the often overlooked area of network devices in the enterprise security model.

Hackers also went after Cisco RV320/RV325 routers, two models very popular among internet service providers and large enterprises, taking advantage of vulnerabilities that allow a remote attacker to get sensitive device configuration details and inject and run admin commands on the device without a password.

And, within the first two weeks of January, 2020 attackers began exploiting Citrix vulnerabilities in the wild, using public proof-of-concept exploit code for CVE-2019-19781, a vulnerability in Citrix enterprise equipment that can allow hackers to take over devices and access a companies' internal networks over the internet, without authentication credentials.

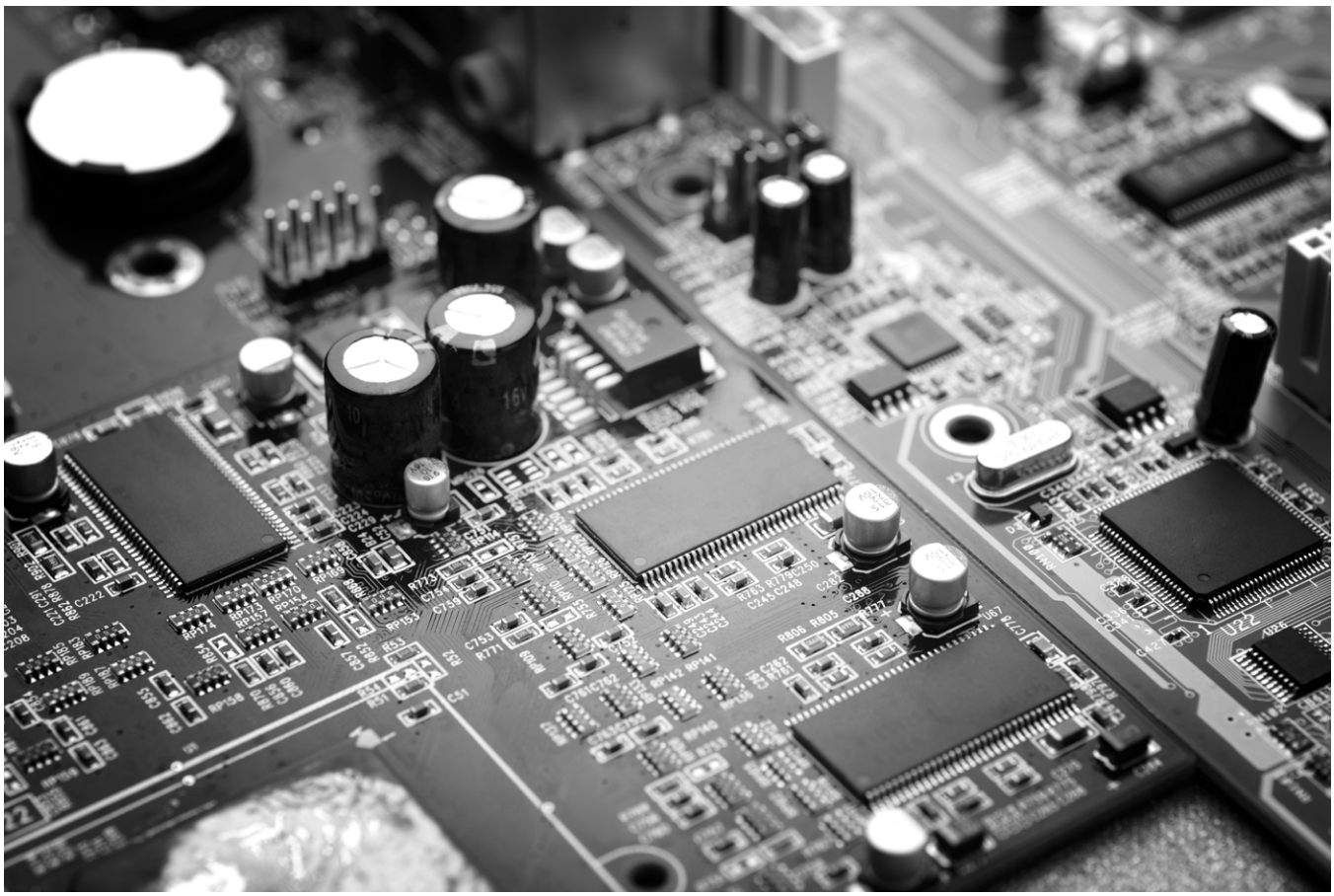
These are just a few examples of how firmware can be attacked. Traditional attacks at the software layer such as malware can be extended to the firmware layer via firmware vulnerabilities or readily available drivers as detailed in our recent analysis. Firmware attacks can also be launched over the network as seen in the JungleSec ransomware and the USB Anywhere research.

Likewise, attacks can also come via physical access using USB, Thunderbolt, PCIe, or other external devices. While these techniques can be applied to any device, they are of particular concern to laptops, which are often exposed to physical attack and can easily be compromised during travel. With just a few minutes of access to a laptop, such as in a hotel room, an attacker could compromise the firmware of the device in a way that would be virtually undetectable by traditional security software.

In all of these cases, an exploit can lead to the installation of a known or unknown firmware implant. This multitude of potential attack vectors and the high impact of a firmware compromises make it critical for organizations to be able to detect threats in this fundamental layer.

☆ RECOMMENDATIONS

- Review existing capabilities to detect firmware attacks and asset tampering, paying particular attention to travel and other high-risk environments. Assess the likelihood of attack and the impact if such attacks go undetected.
- Consider incorporating firmware attacks into planned 2020 red and purple team engagements.
- Add security tools to automatically monitor the integrity of system and component firmware and alert to any compromises.
- Include a combination of whitelisting, threat signatures, and behavioral analysis to detect both known and unknown firmware implants.



3 Do You Have Visibility Into & Control Over Risks in Your Technology Supply Chain?

While most organizations are quite accustomed to dealing with traditional malware and network-based threats, the technology supply chain itself has rapidly emerged as an important threat vector. Compromises in the supply chain can be particularly challenging to catch given the scale that new devices are introduced into most organizations and that initial presumed "good" state of the device may already be compromised. Even after a device is deployed, compromises to a vendor's update process can allow an attacker to take advantage of the trust between an enterprise and its vendors.

To make matters even more complicated, many manufacturers' source components include code from a variety of third-party vendors, which can all be a source of weakness or compromise that affect a multitude of targets. Organizations can easily inherit these risks from a manufacturer or the firmware security issues of their trusted partners, exposing potentially serious impact to devices and operations.

Unfortunately, 2019 once again provided examples of vulnerabilities and attacks in an organization's supply chain:

ShadowHammer Attack: In early 2019 attackers were able to compromise one of the world's largest computer manufacturers, and use the vendor's official update tool to push malware to hundreds of thousands of customers. Specifically, attackers were able to use ASUS's Live Update tool to deliver malware that was validly signed by ASUS. This tool included the ability to update both software and firmware. The potential for completely valid systems to be compromised underscores the importance of behavioral monitoring of firmware to detect actions that inconsistent with normal operations.

Vulnerable Firmware in the Supply Chain of Enterprise Servers: Eclypsium researchers initially discovered a vulnerability in the BMC of a Lenovo ThinkServer. However, further analysis revealed that the underlying issue was due to code from a third party vendor, and the same vulnerability was passed on to a variety of vendors including Gigabyte and Acer.

The complexity of modern technology supply chains means that organizations need the ability to independently verify the safety of their supply chains both in terms of the integrity of firmware as well as evaluating technology for potential weaknesses.

☆ RECOMMENDATIONS

- Add scanning processes to evaluate newly acquired hardware for firmware integrity and the presence of vulnerabilities, particularly for assets that serve critical functions or roles in the organization.
- Establish processes to scan acquired hardware infrastructure during any M&A process.
- Evaluate prospective technology and service providers in terms of firmware security as part of the overall supplier evaluation and due diligence process.
- Regularly monitor firmware behavior to identify malicious or anomalous firmware behaviors.
- Ensure your procurement and vendor engagement programs include assigning responsibility to appropriate parties for the assurance of 3rd party components involved in the delivery or products and services. When delegating responsibility to groups outside your organization, ask for details describing how they manage this risk that you inherit.
- Establish appropriate runbook sections for how your organization will deal with potential issues that extend to your vendors/partners via supply network chain related firmware issues.

4 Are Your SOC and IR Teams Equipped to Deal With Firmware Threats?

As discussed previously, persistence and defense evasion are some of the prime reasons that attackers target firmware in the first place. By infecting the firmware of a device, an attacker can significantly increase the likelihood their code survives a complete re-imaging of the victim system. This toehold can be used to regain control over the system and the new OS and ultimately resume the attack.

This capability has a major impact on the efficacy of both threat hunting as well as how IR teams approach the recovery of compromised devices. Without the ability to verify the integrity of a device's firmware, many traditional device recovery processes could lead to a never-ending cycle of reinfection.

This means that organizations should consider firmware across a wide range of IR-related activities including:

Alerting: Organizations need to understand how the existing alerting infrastructure applies to firmware. Does the SIEM handle firmware-based alerts? Do security solutions generate alerts based on firmware integrity and behavior, malicious add-on devices, and BMC connections?

Forensics and Hunting: Do forensics procedures extend to firmware analysis? Do threat hunters have tools to look for anomalous firmware behavior in the environment? Do hunters have tools to facilitate the analysis of suspicious firmware?

IR Playbooks and Knowledge Base: Are IR teams trained to know when to include firmware as part of their triage and response process? Does the IR knowledge base cover firmware as possible initial infection vectors? Do teams have runbooks before travel devices are reconnected to the network?

Examples from 2019 highlight the critical importance of including firmware as a part of standard IR efforts:

LoJax Malware: While first discovered in 2018, ongoing analysis from NetScout found that LoJax domains were still going strong in 2019. LoJax was one of the first widespread malware campaigns to use firmware for long-term persistence even after re-imaging.

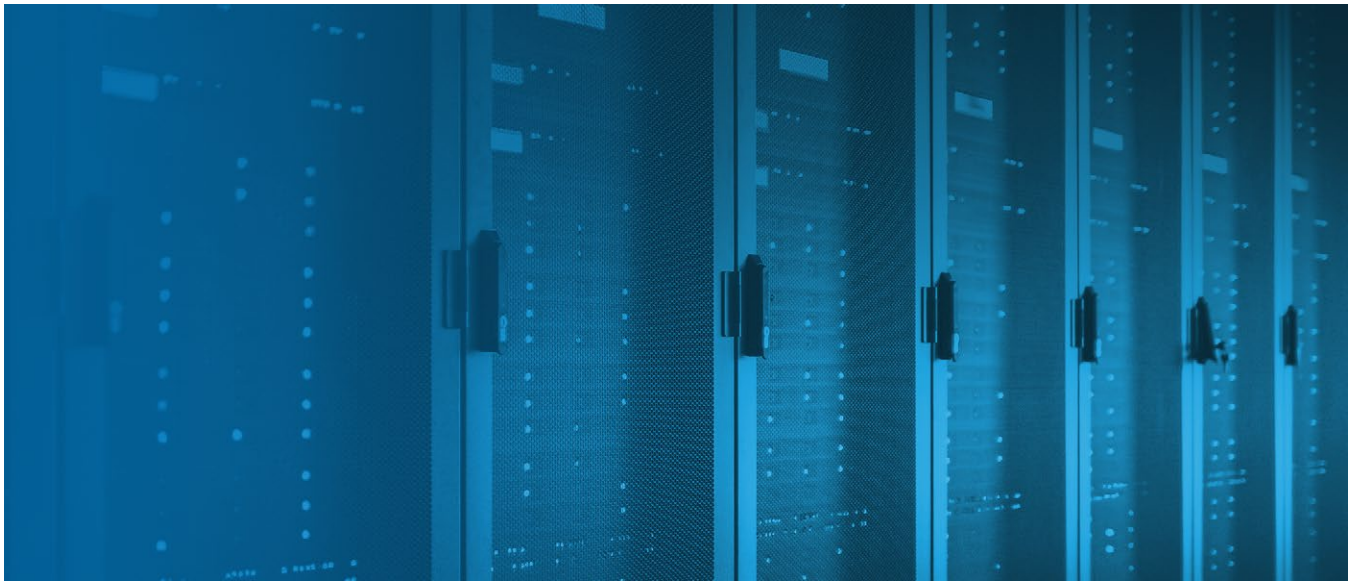
QSnatch Ransomware: As we saw earlier in the example of QSnatch ransomware, the malware specifically targeted the firmware of the victim device and even added measures to ensure that the firmware couldn't be updated.

As other forms of malware continue to adopt this strategy, it makes it evermore important for IR and hunt teams to be able to analyze the firmware of a device.

☆ RECOMMENDATIONS

- Include firmware scanning as a standard component of incident response of devices that are potentially compromised.
- Use firmware scanning to verify the integrity of all firmware before returning a device to service.
- Arm threat hunters with tools that monitor for unusual firmware behavior to further analyze suspicious devices.
- Identify any gaps in how firmware-related alerts are handled both in existing security tools as well as the SIEM.
- Add firmware processes to standard IR triage and response runbooks.
- Evaluate and update the IR Knowledge Base to include firmware-related information.

5 Are You Prepared for Firmware-Related Business Risks?



The rise of firmware security is not limited solely to enterprise security teams. Industry analysts, regulatory bodies, and even the general public have all dedicated increased focus to the firmware layer. This can bring new scrutiny and potential business risks that organizations need to be prepared for.

In recent reports, Gartner and Forrester have both provided stark warnings on the state of firmware security and the risk to enterprises that don't address it. This is a strong indicator that the reach of these threats has grown well beyond the realms of nation-state attacks and hot topics at hacker conferences. And with this added attention, organizations should expect additional questions from management, partners, and customers in terms of how the firmware layer is being secured.

Regulatory compliance is one area where firmware is gaining additional attention. Multiple NIST documents, including the Cybersecurity Framework, heavily focus on the importance of firmware in both the management of risk as well as the implementation of security controls. In response to industry demand, the PCI Security Standards Council published a mapping between PCI DSS v. 3.2.1 and the NIST Cybersecurity Framework v. 1.1. FISMA controls also clearly and repeatedly emphasize the need to secure firmware.

These efforts show that organizations are increasingly looking for ways to standardize their efforts to secure every layer of the technology stack. Given the rise in attention that firmware and hardware related security issues have received, it is no surprise that a spotlight is falling on this aspect of every enterprise network. While the specific implementation of these requirements will naturally vary for each organization, it is important for organizations to clearly understand that firmware and hardware are now a critical part of compliance, both for the organization itself and for any 3rd party suppliers.

☆ RECOMMENDATIONS

- Define and document the role of firmware and firmware security in the organization's security policies, practices, and procedures.
- Review regulatory requirements in terms of hardware and firmware to fully understand the organization's obligations.
- Consider implementing risk management and security controls aimed at the firmware layer of the enterprise.
- Add appropriate language to contracts of vendors who may be considered 3rd party suppliers to your customers and partners.

SUMMARY

Firmware is rapidly becoming a fundamental and essential part of a modern enterprise security practice. Recommendations from industry analysts, changes in industry regulations, and ongoing developments in the vulnerability and threat landscape all indicate the growing importance of firmware security.

We hope that the information in this report provides a practical resource for both understanding the real-world issues that are driving these changes, as well as a way to evaluate your own approach to firmware security. For convenience, these recommendations are available as a separate checklist.

Of course, the included recommendations should not be seen as an exhaustive list of steps related to firmware security. Requirements will naturally vary from organization to organization based on their unique traits and their tolerance for risk. If you would like to learn more about any of the topics in this report, please contact the Eclypsium team at info@eclypsium.com.