Eclypsium

SUPPLY CHAIN SECURITY FOR ENTERPRISE INFRASTRUCTURE_

Trust your tech, from core to cloud.

INTRODUCTION_

Firmware security is a key element of multiple important NIST documents, including SP 800-37 (the Risk Management Framework), SP 800-53 (Security and Privacy Controls), SP 800-147 (BIOS Protection Guidelines), 800-155 (BIOS Integrity Measurement) and 800-193 (Platform Resiliency Guidelines). At a high level, SP 800-37 establishes a lifecycle approach that guides the creation and ongoing administration of a security program. SP 800-53, then provides additional details on the types of controls that may be implemented and considerations for each. Both documents identify firmware as a critical part of the security program and consistently use the phrase “hardware, software, and firmware” when describing the components of technology and devices to be protected. In this brief we outline the NIST requirements that pertain to firmware security and provide guidance for organizations seeking to achieve compliance with these standards.

UNDERSTANDING THE FIRMWARE ATTACK SURFACE_

Eclypsium guidance and considerations: Perform an initial firmware vulnerability assessment of critical devices or assets. Eclypsium can automate the analysis of devices assessing risk and integrity. Firmware analysis should include system-level firmware such as BIOS or UEFI, but should also extend to firmware of hardware components within the system such as drives, processors, and network adapters.

Scans should be able to identify the following:

- **Systems with out of date firmware**
- **Systems with firmware vulnerabilities**
- **Systems with missing hardware protections**

UNDERSTANDING DEVICE RISK AND IMPACT OF THREATS_

Eclypsium guidance and considerations: Organizations may want to consider the impact of firmware-based threats to the following high-value devices during the categorization phase:

High-Value Laptops

While all devices are potentially subject to attacks on their firmware, laptops are exposed more often than other assets. An attacker with physical access to a device can compromise the firmware in 5 minutes. Thus organizations may want to consider firmware security controls for devices that carry high-value information and/or travel to untrusted environments.

Critical Servers

Firmware provides an ideal path to both steal data or deny access to it altogether. This is particularly true of high-value servers. With the complexity and quantity of components (baseboard management controllers, network cards, system firmware, etc.) securing servers that have high privilege and contain critical assets, can be unmanageable.

Networking and Security Gear

Recent large-scale Russian attacks have shown that networking gear presents a particularly powerful prize for attackers. By subverting the network infrastructure, attackers could easily read, manipulate, or even redirect content on the network. Likewise the very network controls charged with securing the network could be targets of attack.

Control	References	Eclypsium Detections
SI—System and Information Integrity SI-2 Flaw Remediation SI-4 Information System Monitoring SI-7 Software, Firmware, and Information Integrity	In-the-wild implants (eg. HackingTeam, Lojax)	**1.** Confirm firmware integrity **2.** Identify insecure firmware and apply updates **3.** Ensure that all firmware updates are cryptographically signed and that devices require any firmware updates to be signed **4.** Monitor devices for signs of malicious firmware behavior **5.** Analyze systems to ensure the integrity of the boot process and boot firmware **6.** Detect firmware threats such as implants, backdoors, and rootkits
SA—System and Services Acquisition SA-12 Supply Chain Protection SA-19 Component Authenticity	Supply chain interdictions	**1.** Evaluate prospective technology for firmware security and avoid products that can be easily modified at the firmware level. **2.** Check all newly acquired devices to confirm the integrity of the firmware **3.** Monitor devices for signs of malicious firmware behavior
CM—Configuration Management CM-2 Baseline Configuration CM-5 Access Restrictions for Change CM-7 Least Functionality	Secure Configuration PLATINUM malware campaign	**1.** Record expected configuration and behavior of device firmware and hardware **2.** Activate firmware and hardware security features **3.** Analyze critical devices to ensure unnecessary features are disabled, particularly remote management interfaces that are not used.
AC—Access Control AC-6 Least Privilege	Firmware Storage Vulnerabilities	**1.** Ensure any unnecessary debug functionality is not enabled **2.** Ensure firmware storage is properly protected
RA—Risk Assessment RA-5 Vulnerability Scanning	Firmware and hardware vulnerabilities (eg. Speculative execution side-channels, vulnerable firmware storage, insecure SMM code)	**1.** Prioritize the analysis and monitoring of firmware and hardware vulnerabilities **2.** Regular scans should be able to identify **a.** Systems with out of date firmware **b.** Systems with firmware vulnerabilities **c.** Systems with missing protections
IR— Incident Response IR-4 Incident Handling IR-10 Security Analysis Team	Attackers using firmware implants to persist across system re-imaging.	**1.** Perform firmware scans of devices related to incident to track scope **2.** Verify integrity of firmware of all affected hosts during system recovery **3.** Arm staff with tools to assist in forensic analysis of firmware-based threats
MA—Maintenance MA-3 Maintenance Tools	BMC, IPMI, and Intel AMT as potential attack vectors	**1.** Monitor management interfaces for vulnerabilities or signs of compromise **2.** Scan management resources for vulnerabilities **3.** Only enable remote management tools for devices that have an operational need

CONCLUSION_

This document highlights some of the areas where firmware security can play an important role in NIST compliance. Firmware integrity is just one part of what a supply chain security solution can provide. The Eclypsium supply chain security platform helps to protect critical hardware, firmware, and software components in your IT infrastructure and covers many controls described in NIST standards. If you have any questions or concerns related to topics in this document, please contact the Eclypsium team at info@eclypsium.com.