AMI Meridian™

Vulnerability Management Service (VMS)

Increasing Challenge of CVE Mitigation

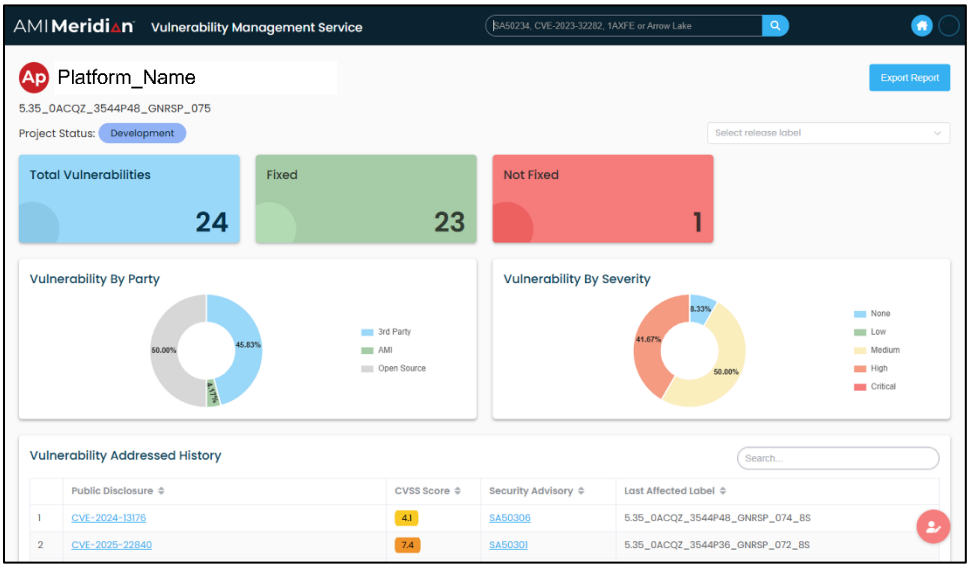
The list of vulnerabilities in software and firmware has experienced exponential growth, with over 40,000 CVEs published in 2024—a 38% increase from 2023's 28,818. This surge, averaging 108 new CVEs daily, complicates tracking and patching efforts for code used in existing products. Notably, 768 CVEs were exploited in the wild in 2024, up 20% from the previous year. This escalating volume and exploitation rate challenge security teams to prioritize and address vulnerabilities effectively.

With the surge in CVEs, applications that track vulnerabilities relevant to firmware projects are essential. By leveraging a product's Software Bill of Materials (SBOM), these tools can map known CVEs to specific components. This targeted approach streamlines vulnerability management, helping teams quickly identify and mitigate security risks hidden within third-party libraries or dependencies used in firmware.

Features:

- CVE reporting with status and severity metrics
- Vulnerability lookup and tracking against affected platforms and products
- Links to original Nation Vulnerability Database report
- Matching Security Advisory details and document link
- Statistical export to XLS workbook
- Provides streamlined path for developers analyzing SBOMs for vulnerabilities

Figure 1: AMI Meridian VMS User Interface



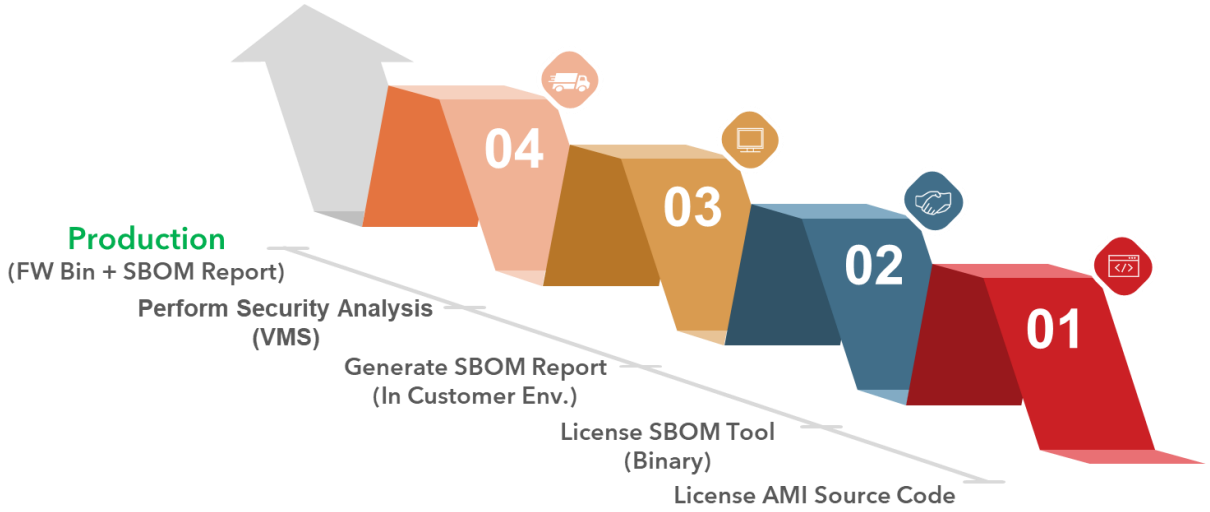
AMI Meridian VMS

To better facilitate mitigation of CVEs affecting platform code, AMI offers the Meridian Vulnerability Management Service (VMS). Built into the AMI Meridian cloud-based services platform, VMS provides tracking for CVEs affecting different platform firmware packages. Through a simplified user interface, system builders and end users can track the vulnerabilities affecting their firmware and align to the best possible release or update. Figure 1 provides a view of the VMS User Interface.

AMI Meridian VMS and SBOM

AMI VMS is a critical component for diligent code integration and management. One way VMS is used as part of the development cycle is to perform a security analysis on SBOM components. AMI helps to facilitate this flow through its SBOM utilities offered with AMI Aptio and MegaRAC firmware. Once the SBOM utilities are licensed, developers can generate the relevant SBOM report and run it against the CVEs for their platform, revealing any components that may contain vulnerabilities. Combining the AMI SBOM utilities with VMS streamlines the development flow while being prudent about firmware security. Figure 2 shows the high-level flow for SBOM analysis using VMS.

Figure 2: Flow for VMS SBOM Analysis



For more information, please visit the request form at ami.com/contact