Dear Customers and Partners:

At AMI, we recognize the critical importance of addressing security issues in the firmware supply chain. It's crucial to understand the downstream impacts that such issues can have, not only on individual systems but on the entire ecosystem. That's why we continue to be proactive to enhance security and transparency. Our advisories exemplify AMI's security stewardship in the firmware supply chain as AMI continues to create Common Vulnerabilities and Exposures (CVEs) for vulnerabilities. By doing this, we're not only addressing a specific vulnerability but also contributing to a culture of accountability and collaboration in the industry.

We remain dedicated to working closely with the open-source software (OSS) community to uphold best practices in issuing formal CVEs and implementing mitigations for code remediation. Our goal is to empower the entire supply chain to collectively enhance its security posture.

We want to make it very clear that if OSS code providers adhere to minimum security protocols like CVEs, the risk of a "Forever Vulnerability" significantly diminishes. This underscores the importance of industry-wide collaboration and adherence to security standards.

Finally, AMI strongly advises all security research firms to follow global Product Security Incident Response Team (PSIRT) best practices. Coordinating findings with supply chain vendors before public announcements is crucial to prevent zero-day vulnerabilities from being exploited and exposing systems unnecessarily to threat actors before effective fixes are available. This proactive approach can help mitigate risks and protect the integrity of supply chain systems. At AMI, we remain committed to driving positive change in cybersecurity practices and fostering a secure and resilient supply chain environment for all stakeholders.

Yours Truly,
Sam Cure
AMI Chief Information Security Officer (CISO)

3095 Satellite Boulevard | Building 800, Suite 425 | Duluth, Georgia 30096
www.ami.com