AMI Security Advisory

OSS Vulnerability - MegaRAC SPX

ID: AMI-SA-2024002 | April 15, 2024

INTRODUCTION

At AMI, we recognize the critical importance of addressing security issues in the supply chain of firmware. 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've taken proactive steps to enhance security and transparency.

This advisory exemplifies AMI's security stewardship in the FW supply chain as AMI has created a CVE for a vulnerability in the lighttpd open-source software (OSS) module which was mitigated silently by the maintainer with a patch dating back to 2018, without responsibly advising on it by creating a CVE. By doing so, we're not only addressing a specific vulnerability but also contributing to a culture of accountability and collaboration in the industry.

Moving forward, we remain dedicated to working closely with open-source software 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 enhance its security posture collectively.

It's worth emphasizing 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.

In addition, we strongly advise 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.

SECURITY VULNERABILITIES AND REMEDIATION INFORMATION

Vulnerability	CVSS Vector	CVSS Score	CWE	Fix Version
CVE-2024-3708	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.7	CWE-113	TBD
				TBD

Change History

Date	Revision	Description
4-15-2024	1.00	First publication of document

For additional information AMI Security Center or email mediasecurityinqueries@ami.com