January 12, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of reported potential security vulnerabilities in AMI MegaRAC SP-X Baseboard Management Controllers that could lead to stack overflow, stack memory corruption, heap memory corruption and untrusted pointer dereference vulnerabilities. The vulnerabilities affect Baseboard Management Controllers (BMC) - ThinkSystem HR610X prior to V15.41, ThinkSystem HR630X/HR650X prior to V11.54, ThinkSystem HR630X_V2 prior to V1.26, ThinkSystem HR630X/HR650X prior to V11.54, ThinkSystem HG680X prior to SR590V2 V6.41.00, SR660V2 V6.93.00, WR5220G3 V6.47.00, and Lenovo ThinkSystem SR635/655 prior to AMBT50N.

Technical Details

AMI reported potential security vulnerabilities in AMI MegaRAC SP-X Baseboard Management Controllers that could lead to stack overflow, stack memory corruption, heap memory corruption and untrusted pointer dereference vulnerabilities.

AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a stack-based buffer overflow via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.

- AMI recommends customers upgrade to the BMC firmware version (or newer) indicated for your model in the Product Impact section below.
- AMI also recommends that customers continue to maintain strict access controls to BMC devices.

AMI has released AMI MegaRAC SP-X security enhancements to address these vulnerabilities.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-37293, CVE-2023-37297, CVE-2023-37296, CVE-2023-37295, CVE-2023-37294, CVE-2023-3043, CVE-2023-34333
- LEN-135372 AMI MegaRAC Vulnerabilities
- VRM Vulnerability Reports