



AMI Security Advisory

May 1, 2023, SLP DoS Attack – MegaRAC SPX

ID: AMI-SA-2023004 | May 1, 2023

INTRODUCTION

The Service Location Protocol SLP does not support authentication or perform any restrictions on the ability to register a new service. This can be leveraged by an attacker to perform UDP-based denial-of-service attacks with a high amplification factor.

SECURITY VULNERABILITIES

April 2023:

CVE-2023-29552: SLP_DoS_Attack

REMEDIATION INFORMATION

Vulnerability	CVSS Vector	Base Score	Fix Version
CVE-2023-29552	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.5	SPx_12:Disabled SPx_13:Does not support

Note: A score has not yet been assigned to this issue on NVD but based on the impact we have assigned the above score.

Change History

Date	Revision	Description
5-01-2023	1.00	First publication of document