AMI Security Advisory

Jan. 30, 2023 Eclypsium Vulnerabilities – MegaRAC SPX

AMI Advisory ID: AMI-SA-2023001 | January 30, 2023

INTRODUCTION

AMI was recently notified of five vulnerabilities that affect AMI products. Three were published in December 2022, and the remaining two are covered in this advisory. The external researcher who identified these is Vlad Babkin of Eclypsium Research.

SECURITY VULNERABILITIES

January 2023:

CVE-2022-40258: Weak Password Hashes for Redfish & API

CVE-2022-26872: Password Reset Interception via API

December 2022:

CVE-2022-40259: Redfish Arbitrary Code

CVE-2022-2827: User Enumeration

CVE-2022-40242: Default Credentials

REMEDIATION INFORMATION

Vulnerability	CVSS Vector	CVSS Score	Fix Version
CVE-2022-40258	CVSS:3.1/ AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3	SPx_12-update-7.00
			SPx_13-update-5.00
CVE-2022-26872	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H	8.3	SPx12-update-7.00
			SPx13-update-5.00
CVE-2022-40259	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	9.9	SPx12-update-7.00
			SPx13-update-5.00
CVE-2022-2827	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5	SPx12-update-7.00
			SPx13-update-5.00
CVE-2022-40242	CVSS:3.1/ AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H	8.3	SPx12-update-7.00
			SPx13-update-5.00

Change History

Date	Revision	Description
1-30-2023	1.00	First publication of document
2-01-2023	2.00	Updated CVSS Info for CVE-2022-40242, CVE-2022-40259