AMI Security Advisory

Feb. 14,2023 Redfish Authentication Vulnerabilities – MegaRAC SPX

AMI Advisory ID: AMI-SA-2023002 | February 14, 2023

Advisory: Two authentication vulnerabilities that could be exploited through the Redfish feature of AMI's MegaRAC SPX BMC product.

CVE(S)

Vulnerability 1:

CVE-2023-25191: Password Disclosure through Redfish

Vulnerability 2:

CVE-2023-25192: User Enumeration through Redfish

Identifier: Intel's DCG Red Team.

REMEDIATION INFORMATION

Vulnerability	CVSS Vector	CVSS Score	Fix Version
CVE-2023-25191	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	9.1	SPx_12-update-7.00
			SPx_13-update-5.00
CVE-2023-25192	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3	SPx12-update-7.00
			SPx13-update-5.00

Change History

Date	Revision	Description
2-14-2023	1.00	First publication of document