SSA-702935: Redfish Server Vulnerability in maxView Storage Manager

Publication Date:	2024-01-09
Last Update:	2024-01-09
Current Version:	V1.0
CVSS v3.1 Base Score:	10.0

SUMMARY

MaxView Storage Manager shipped with affected SIMATIC IPCs contains a Redfish Server Vulnerability that could provide unauthorized access.

Microchip has released new versions for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC IPC647E: All versions with maxView Storage Manager < V4.14.00.26068 on Windows	Update maxView Storage Manager to V4.14.00.26068 or later version https://storage.microsemi.com/en-us/support/raid/sas_raid/asr-3151-4i/
SIMATIC IPC847E: All versions with maxView Storage Manager < V4.14.00.26068 on Windows	Update maxView Storage Manager to V4.14.00.26068 or later version https://storage.microsemi.com/en-us/support/raid/sas_raid/asr-3151-4i/
SIMATIC IPC1047E: All versions with maxView Storage Manager < V4.14.00.26068 on Windows	Update maxView Storage Manager to V4.14.00.26068 or later version https://storage.microsemi.com/en-us/support/raid/sas_raid/asr-3151-4i/

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

SIMATIC IPC (Industrial PC) is the hardware platform for PC-based automation from Siemens.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2023-51438

In default installations of maxView Storage Manager where Redfish® server is configured for remote system management, a vulnerability has been identified that can provide unauthorized access.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ADDITIONAL INFORMATION

For additional information see also the Microchip vendor statement.

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2024-01-09):	Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.