SSA-794542: Insecure Folder Permissions in SIMARIS Configuration

Publication Date: 2021-02-09
Last Update: 2021-05-11
Current Version: V1.1
CVSS v3.1 Base Score: 4.4

SUMMARY

The installation of SIMARIS configuration causes insecure folder permissions that could allow vertical privilege escalation.

Siemens has released an update for SIMARIS and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMARIS configuration: All versions < V4.0.1	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109740118/

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Set installation path to a folder inside %APPDATA% for your user.
- Apply the principle of least privileges operation of SIMARIS configuration and especially do not use any administrative accounts for executing the software.

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

The SIMARIS configuration software supports a fully digital engineering process when building distribution systems, from planning to cost calculation and bid preparation to documentation of distribution systems in compliance with the standards.

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-2020-28392

During installation to default target folder, incorrect permissions are configured for the application folder and subfolders which could allow an attacker to gain persistence or potentially escalate privileges should a user with elevated credentials log onto the machine.

CVSS v3.1 Base Score	4.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-276: Incorrect Default Permissions

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Richard Davy from ECSC Group for coordinated disclosure

ADDITIONAL INFORMATION

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 (2021-02-09): Publication Date
V1.1 (2021-05-11): Added solution

TERMS OF USE