SSA-386812: Remote Code Execution Vulnerability in Simcenter Amesim before V2021.1

Publication Date: 2023-10-10
Last Update: 2023-10-10
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Simcenter Amesim contains a vulnerable SOAP endpoint that could allow an unauthenticated remote attacker to perform DLL injection and execute arbitrary code in the context of the affected application process.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Simcenter Amesim: All versions < V2021.1	Update to V2021.1 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Limit ports 40002 to 41000 to be accessible only from localhost

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

Simcenter Amesim is an integrated, scalable system simulation platform, allowing system simulation engineers to virtually assess and optimize the performance of mechatronic systems.

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-2023-43625

The affected application contains a SOAP endpoint that could allow an unauthenticated remote attacker to perform DLL injection and execute arbitrary code in the context of the affected application process.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-94: Improper Control of Generation of Code ('Code Injection')

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Guillaume Orlando for reporting the vulnerability

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 (2023-10-10): Publication Date

TERMS OF USE