

SSA-173615: Multiple PAR and ASM File Parsing Vulnerabilities in Solid Edge

Publication Date: 2021-07-13
Last Update: 2021-07-13
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

Siemens has released version SE2021MP5 for Solid Edge to fix multiple heap based buffer overflow vulnerabilities that could be triggered when the application read files in PAR or ASM file formats. If a user is tricked to open a malicious file with the affected application, this could lead to a crash, and potentially also to arbitrary code execution.

Siemens recommends to update to the latest version and to avoid opening of untrusted files from unknown sources.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Solid Edge SE2021: All Versions < SE2021MP5	Update to SE2021MP5 or later version https://support.sw.siemens.com/ (login required)

WORKAROUNDS AND MITIGATIONS

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

- Avoid to open untrusted files from unknown sources in Solid Edge

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

Solid Edge is a portfolio of software tools that addresses various product development processes : 3D design, simulation, manufacturing and design management.

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-2021-34326

The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13422)

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2021-34327

The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing ASM files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13423)

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2021-34328

The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13424)

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2021-34329

The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13427)

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative 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 (2021-07-13): 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.