# SSA-979834: Multiple vulnerabilities in Solid Edge

Publication Date: 2021-01-12
Last Update: 2021-01-15
Current Version: V1.1
CVSS v3.1 Base Score: 7.8

## SUMMARY

Solid Edge is affected by multiple vulnerabilities that could allow arbitrary code execution on an affected system. Siemens has released an update for Solid Edge and recommends to update to the latest version.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| Solid Edge SE2020:<br>All Versions < SE2020MP12 | Update to Version SE2020MP12 or later<br>https://support.sw.siemens.com/ (login required) |
| Solid Edge SE2021:<br>All Versions < SE2021MP2 | Update to Version SE2021MP2 or later<br>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:

- Siemens recommends to limit opening of untrusted files from unknown sources in Solid Edge
- Applying a Defense-in-Depth concept can help to reduce the probability that untrusted code is run on the system. Siemens recommends to apply the Defense-in-Depth concept: https://www.siemens.com/industrialsecurity

## 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-2020-28381

Affected applications lack proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write into uninitialized memory. An attacker could leverage this vulnerability to execute code in the context of the current process.

| | |
|---|---|
| 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-787: Out-of-bounds Write |

Vulnerability CVE-2020-28382

Affected applications lack proper validation of user-supplied data when parsing PAR files. This could result in a out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process.

| | |
|---|---|
| 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-787: Out-of-bounds Write |

Vulnerability CVE-2020-28383

Affected applications lack proper validation of user-supplied data when parsing PAR files. This can result in an out of bounds write past the memory location that is a read only image address. An attacker could leverage this vulnerability to execute code in the context of the current process.

| | |
|---|---|
| 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-787: Out-of-bounds Write |

Vulnerability CVE-2020-28384

Affected applications lack proper validation of user-supplied data when parsing PAR files. This could lead to a stack based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process.

| | |
|---|---|
| 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-121: Stack-based Buffer Overflow |

Vulnerability CVE-2020-28386

Affected applications lack proper validation of user-supplied data when parsing DFT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process.

| | |
|---|---|
| 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-787: Out-of-bounds Write |

Vulnerability CVE-2020-26989

Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a stack based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process.

| | |
|---|---|
| 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-121: Stack-based Buffer Overflow |

## ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure
- Industrial Control System Cyber Emergency Response Team (ICS-CERT) for coordination efforts

## 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 (2021-01-12): Publication Date
V1.1 (2021-01-15): Added additional fix version for SolidEdge SE2020

## TERMS OF USE