SSA-574442: Multiple PAR and DFT File Parsing Vulnerabilities in Solid Edge

Publication Date: 2021-04-13
Last Update: 2021-06-08
Current Version: V1.1
CVSS v3.1 Base Score: 7.8

SUMMARY

Siemens has released a new version for Solid Edge to fix multiple vulnerabilities that could be triggered when the application reads files in different file formats (PAR, DFT extensions). 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 or data extraction on the target host system.

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 SE2020: All versions < SE2020MP13	Update to SE2020MP13 or later version https://support.sw.siemens.com/ (login required)
Solid Edge SE2020: All versions < SE2020MP14 only affected by CVE-2020-26997, CVE-2021-25678, CVE-2021-27382	Update to SE2020MP14 or later version https://support.sw.siemens.com/ (login required)
Solid Edge SE2021: All Versions < SE2021MP4	Update to SE2021MP4 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-2020-28385

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. (ZDI-CAN-12049)

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-2020-26997

Affected applications lack proper validation of user-supplied data when parsing PAR files. This could lead to pointer dereferences of a value obtained from untrusted source. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11919)

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-822: Untrusted Pointer Dereference

Vulnerability CVE-2021-25678

Affected applications lack proper validation of user-supplied data when parsing PAR 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. (ZDI-CAN-12529)

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-2021-27380

Affected applications lack proper validation of user-supplied data when parsing PAR 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. (ZDI-CAN-12532)

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-2021-27382

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. (ZDI-CAN-13040)

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
- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts

ADDITIONAL INFORMATION

For more details regarding the vulnerabilities CVE-2020-28385 and CVE-2021-27380 for fix SE2020MP13 refer to: - SSA-715184

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 (2021-04-13):	Publication Date
V1.1 (2021-06-08):	Updated remediation for CVE-2020-26997, CVE-2021-25678 and CVE-2021-27382

TERMS OF USE