



CVE-2020-28385

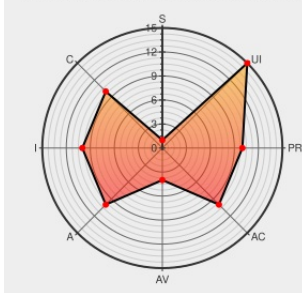
Published on: 03/15/2021 12:00:00 AM UTC

Last Modified on: 12/10/2021 09:36:00 PM UTC

CVE-2020-28385

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Solid Edge](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in Solid Edge SE2020 (All versions < SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP4). 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)

CVE-2020-28385 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [S](#) Siemens - Solid Edge SE2020 version All versions < SE2020MP13

Affected Vendor/Software: [S](#) Siemens - Solid Edge SE2021 version All Versions < SE2021MP4

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Siemens Solid Edge File Parsing CISA	us-cert.cisa.gov text/html	CONFIRM us-cert.cisa.gov/ics/advisories/icsa-21-103-06
	Vendor Advisory cert-portal.siemens.com application/pdf	MISC cert-portal.siemens.com/productcert/pdf/ssa-715184.pdf
	cert-portal.siemens.com application/pdf	CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-574442.pdf

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Known Affected Configurations (CPE V2.3)

cpe:2.3:a:siemens:solid_edge:se2020:maintenance_pack1:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2020:maintenance_pack10:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2020:maintenance_pack11:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2020:maintenance_pack12:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2020:maintenance_pack2:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2020:maintenance_pack3:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2020:maintenance_pack4:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2020:maintenance_pack5:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2020:maintenance_pack6:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2020:maintenance_pack7:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2020:maintenance_pack8:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2020:maintenance_pack9:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2021:-::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2021:maintenance_pack1:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2021:maintenance_pack2:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2021:maintenance_pack3:~::~~::~~::~~::~~::~~::
cpe:2.3:a:siemens:solid_edge:se2021:mp3:~::~~::~~::~~::~~::~~::

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
← Previous ID Next ID→		