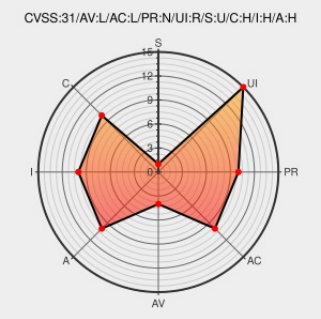
CVE-2020-28386

Published on: 01/12/2021 12:00:00 AM UTC

Last Modified on: 12/10/2021 09:44:00 PM UTC

CVE-2020-28386

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Solid Edge from Siemens contain the following vulnerability:

A vulnerability has been identified in Solid Edge SE2020 (All Versions < SE2020MP12), Solid Edge SE2021 (All Versions < SE2021MP2). 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.

CVE-2020-28386 has been assigned by productcert@siemens.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Siemens** - **Solid Edge SE2020** version **All Versions < SE2020MP12**

Affected Vendor/Software: **Siemens** - **Solid Edge SE2021** version **All Versions < SE2021MP2**

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
ZDI-21-060 | Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-21-060/
ZDI-21-077 | Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-21-077/
Siemens Solid Edge | CISA	Third Party Advisory US Government Resource us-cert.cisa.gov text/html	MISC us-cert.cisa.gov/ics/advisories/icsa-21-012-04
	Vendor Advisory cert-portal.siemens.com application/pdf	MISC cert-portal.siemens.com/productcert/pdf/ssa-979834.pdf

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Siemens	Solid Edge	All	All	All	All
Application	Siemens	Solid Edge	se2020	-	All	All
Application	Siemens	Solid Edge	se2020	maintenance_pack1	All	All
Application	Siemens	Solid Edge	se2020	maintenance_pack10	All	All
Application	Siemens	Solid Edge	se2020	maintenance_pack11	All	All
Application	Siemens	Solid Edge	se2020	maintenance_pack2	All	All
Application	Siemens	Solid Edge	se2020	maintenance_pack3	All	All
Application	Siemens	Solid Edge	se2020	maintenance_pack4	All	All
Application	Siemens	Solid Edge	se2020	maintenance_pack5	All	All
Application	Siemens	Solid Edge	se2020	maintenance_pack6	All	All
Application	Siemens	Solid Edge	se2020	maintenance_pack7	All	All
Application	Siemens	Solid Edge	se2020	maintenance_pack8	All	All
Application	Siemens	Solid Edge	se2020	maintenance_pack9	All	All
Application	Siemens	Solid Edge	se2021	-	All	All
Application	Siemens	Solid Edge	se2021	maintenance_pack1	All	All
Application	Siemens	Solid Edge	se2021	mp1	All	All

Application	Siemens	Solid Edge	se2021	mp1	All	All
Application	Siemens	Solid Edge	All	All	All	All

cpe:2.3:a:siemens:solid_edge:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:solid_edge:se2020:-:*:*:*:*:*:*:

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_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:mp1:*:*:*:*:*:*:

cpe:2.3:a:siemens:solid_edge:se2021:mp1:*:*:*:*:*:*:

cpe:2.3:a:siemens:solid_edge:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report