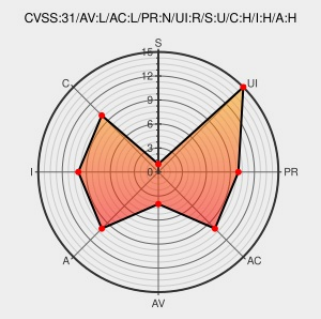
CVE-2022-37864

Published on: Not Yet Published

Last Modified on: 10/12/2022 01:47:00 PM UTC

CVE-2022-37864

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 (All Versions < SE2022MP9). The affected application contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted DWG files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17627)

CVE-2022-37864 has been assigned by productcert@siemens.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Siemens** - **Solid Edge** version **All Versions < SE2022MP9**

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

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	MISC cert-portal.siemens.com/productcert/pdf/ssa-258115.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.

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	se2020	-	All	All
Application	Siemens	Solid Edge	se2020	maintenance_pack1	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

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_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:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-37864 : A vulnerability has been identified in Solid Edge All Versions < SE2022MP9 . The affected applica… twitter.com/i/web/status/1…	2022-10-11 10:24:56
/r/netcve	CVE-2022-37864	2022-10-11 10:38:25

← Previous ID

Next ID→

© CVE.report 2023 | Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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