TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
1/14/2021

SUBJECT:
Multiple Vulnerabilities in Siemens Solid Edge Visualization Could Lead to Arbitrary Code Execution (ICSA-21-012-04)

OVERVIEW:
Multiple vulnerabilities have been discovered in Siemens' Solid Edge, the most severe of which could allow for arbitrary code execution in the context of the system process. Solid Edge is used for designing and viewing 2D and 3D models. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Solid Edge versions prior to 2021MP2

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Siemens' Solid Edge, the most severe of which could allow for arbitrary code execution in the context of the system process. Exploits can be triggered by an unsuspecting user opening a malicious file with the vulnerable software.

Details of the vulnerabilities are as follows:

- An out-of-bounds write error when parsing 'PAR' files due to a failure to properly validate user input (CVE-2020-28381, CVE-2020-28382, CVE-2020-28383)
- A stack-based buffer-overflow when parsing 'PAR' files (CVE-2020-28384 and CVE-2020-26989)
- An out-of-bounds write error when parsing 'DFT' files (CVE-2020-28386)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:

- Install the updates provided by Siemens immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services; run all software as a nonprivileged user with minimal access rights.

REFERENCES:
Siemens:
https://cert-portal.siemens.com/productcert/pdf/ssa-979834.pdf

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26989
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28381
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28382
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28383
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28384
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28386

US-CERT:
https://us-cert.cisa.gov/ics/advisories/icsa-21-012-04