The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
10/01/2021

SUBJECT:
Multiple Vulnerabilities in SiemensSolid Edge Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in SiemensSolid Edge, the most severe of which could allow an attacker to cause an arbitrary code execution. Siemens Edge is a portfolio of software tools that addresses various product development processes: 3D design, simulation, manufacturing and design management. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user, an attacker could then view or modify data, as well as take full control of the system.

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

SYSTEMS AFFECTED:
- Solid Edge SE2021: All versions prior to SE2021MP8

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 SiemensSolid Edge, the most severe of which could allow for arbitrary code execution in the context of the system.

Details of the vulnerabilities are as follows:
- Application contains a use-after-free vulnerability that could cause arbitrary code execution. (CVE-2021-37202)

- Application contains an out-of-bounds read while parsing user supplied IFC files which could result in a denial-of-service condition or reading of sensitive information from memory. (CVE-2021-37203)
- Application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files which leads to information leak. (CVE-2021-41533, CVE-2021-41534)
- Application contains a use-after-free vulnerability while parsing OBJ files which leads to arbitrary code execution. (CVE-2021-41535, CVE-2021-41536, CVE-2021-41537)
- Application is vulnerable to information disclosure by unexpected access to an uninitialized pointer while parsing user-supplied OBJ files which leads to information leak. (CVE-2021-41538)
- Application contains a use-after-free vulnerability while parsing OBJ files which leads to arbitrary code execution. (CVE-2021-41539, CVE-2021-41540)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the system. Depending on the privileges associated with the user, an attacker could then view or modify data, as well as take full control of the system.

RECOMMENDATIONS:
The following actions should be taken:

- Install the updates provided by Siemens immediately after appropriate testing.
- Verify that all hosts with a public IP do not have open ports unless absolutely necessary.
- Apply the Principle of Least Privilege to all systems and services.
- Avoid opening files from unknown sources in Solid Edge.

REFERENCES:
Siemens:
https://cert-portal.siemens.com/productcert/pdf/ssa-728618.pdf

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37202
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37203
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41533
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41534
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41535
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41536
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41537
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41538
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41539
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41540