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
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:
1/13/2021

SUBJECT:
Multiple Vulnerabilities in Siemens JT2Go and Teamcenter Visualization Could Lead to Arbitrary Code Execution (ICSA-21-012-03)

OVERVIEW:
Multiple vulnerabilities have been discovered in Siemens' JT2Go and Teamcenter Visualization products, the most severe of which could allow for arbitrary code execution in the context of the system process. JT2Go and Teamcenter Visualization are used for viewing 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:
- JT2Go versions prior to 13.1.0
- Teamcenter Visualization versions prior to 13.1.0

Note: version 13.1.0 of JT2Go and Teamcenter Visualization is vulnerable to the following:
- CVE-2020-26989
- CVE-2020-26990
- CVE-2020-26991

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' JT2Go and Teamcenter Visualization products, 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 XML External Entity injection vulnerability (CVE-2020-26981)
- An out-of-bounds write error when parsing 'CG4' and 'CGM' files (CVE-2020-26982 and CVE-2020-26996)
- An out-of-bounds write error when parsing 'JT' files (CVE-2020-26984)
- An out-of-bounds write error when parsing 'PAR' files (CVE-2020-26988 and CVE-2020-28383)
- An out-of-bounds write error when parsing 'PDF' files (CVE-2020-26983)
- An out-of-bounds write error when parsing 'RGB' and 'SGI' files (CVE-2020-26995)
- A heap-based buffer-overflow when parsing 'JT' files (CVE-2020-26986)
- A heap-based buffer-overflow when parsing 'PCX' files (CVE-2020-26994)
- A heap-based buffer-overflow when parsing 'RGB' and 'SGI' files (CVE-2020-26985)
- A heap-based buffer-overflow when parsing 'TGA' files (CVE-2020-26987)
- A stack-based buffer-overflow when parsing 'CGM' files (CVE-2020-26992 and CVE-2020-26993)
- A stack-based buffer-overflow when parsing 'PAR' files (CVE-2020-26989)
- A type-confusion vulnerability when parsing JT files (CVE-2020-26980)
- A type-confusion vulnerability when parsing 'ASM' files (CVE-2020-26990)
- An untrusted pointer dereference when parsing 'ASM' files (CVE-2020-26991)

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-622830.pdf

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26980

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26981
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26982
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26983
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26984
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26985
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26986
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26988
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26989
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26990
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26991
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26992
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26993
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26994
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26995
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26996
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28383

US-CERT:
https://us-cert.cisa.gov/ics/advisories/icsa-21-012-03