## Severity

Medium

## Analysis Summary

### CVE-2022-29028 CVSS:3.3

Siemens JT2Go and Teamcenter Visualization is vulnerable to a denial of service, caused by an infinite loop condition in the Tiff_Loader.dll dynamic link library when parsing TIFF files. By persuading a victim to open a specially-crafted TIFF file, a remote attacker could exploit this vulnerability to cause a denial of service.

### CVE-2022-29029 CVSS:3.3

Siemens JT2Go and Teamcenter Visualization is vulnerable to a denial of service, caused by a NULL pointer dereference in the CGM_NIST_Loader.dll dynamic link library when parsing CGM files. By persuading a victim to open a specially-crafted CGM file, a remote attacker could exploit this vulnerability to cause a denial of service.

### CVE-2022-29030 CVSS:3.3

Siemens JT2Go and Teamcenter Visualization is vulnerable to a denial of service, caused by an integer overflow in the Mono_Loader.dll dynamic link library when parsing TG4 files. By persuading a victim to open a specially-crafted TG4 file, a remote attacker could exploit this vulnerability to cause a denial of service.

### CVE-2022-29031 CVSS:3.3

Siemens JT2Go and Teamcenter Visualization is vulnerable to a denial of service, caused by a NULL pointer dereference in the CGM_NIST_Loader.dll dynamic link library when parsing CGM files. By persuading a victim to open a specially-crafted CGM file, a remote attacker could exploit this vulnerability to cause a denial of service.

### CVE-2022-29032 CVsS:7.8

Siemens JT2Go and Teamcenter Visualization could allow a remote attacker to execute arbitrary code on the system, caused by a double free in the CGM_NIST_Loader.dll dynamic link library when parsing CGM files. By persuading a victim to open a specially-crafted CGM file, an attacker could exploit this vulnerability to execute arbitrary code on the system.

### CVE-2022-29033 CVsS:7.8

Siemens JT2Go and Teamcenter Visualization could allow a remote attacker to execute arbitrary code on the system, caused by an uninitialized pointer free in CGM_NIST_Loader.dll dynamic link library when parsing CGM files. By persuading a victim to open a specially-crafted CGM file, an attacker could exploit this vulnerability to execute arbitrary code on the system.

## Impact

- Denial of Service
- Code Execution

## Indicators Of Compromise

### CVE

- CVE-2022-29028
- CVE-2022-29029
- CVE-2022-29030
- CVE-2022-29031

- CVE-2022-29032
- CVE-2022-29033

## Affected Vendors

- Siemens

## Affected Products

- Siemens JT2Go
- Siemens Teamcenter Visualization 13.3
- Siemens Teamcenter Visualization 14.0

## Remediation

Refer to Siemens Security Advisory for patch, upgrade or suggested workaround information.

Siemens Security Advisory