SSA-824889: XML File Parsing Vulnerabilities in JT Open and PLM XML SDK

Publication Date: 2024-07-09
Last Update: 2024-07-09
Current Version: V1.0
CVSS v3.1 Base Score: 7.8
CVSS v4.0 Base Score: 7.3

SUMMARY

JT Open Toolkit and PLM XML SDK are affected by stack buffer overflow and null pointer dereference vulnerabilities that could be triggered while parsing XML file. If a user is tricked to open a malicious XML file with any of the affected products, this could cause the application to crash or potentially lead to arbitrary code execution.

Siemens has released new versions for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
JT Open: All versions < V11.5 affected by all CVEs	Update to V11.5 or later version https://support.sw.siemens.com/product/259259756/ See further recommendations from section Workarounds and Mitigations
PLM XML SDK: All versions < V7.1.0.014 affected by all CVEs	Update to V7.1.0.014 or later version https://support.sw.siemens.com/product/242354484/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- CVE-2024-37996, CVE-2024-37997: Do not open untrusted XML files in affected applications

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

JT Open Toolkit is an application programming interface (API) for developers of JT-enabled software. The JT Open Toolkit is a read/write toolkit that enables consistent access to JT file content.

PLM XML SDK is a lightweight, flexible mechanism for transporting product data. It supports an adapter based approach to converting data from any source into XML representations.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2024-37996

The affected applications contain a null pointer dereference vulnerability while parsing specially crafted XML files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L
CVSS v4.0 Base Score	4.8
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2024-37997

The affected applications contain a stack based overflow vulnerability while parsing specially crafted XML files. This could allow an attacker to execute code in the context of the current process.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-121: Stack-based Buffer Overflow

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2024-07-09): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.