tts

tts performance suite

CVE-2022-34169

4. August 2022

tts

Inhaltsverzeichnis

1 Security postmortem for CVE-2022-34169

1.1 Incident date(s)

NVD published date: 2022-07-19
NVD updated criticality date: 2022-07-28

1.2 Authors

tts Digital Adoption Solutions - Development

1.3 Status

Final

1.4 Summary

A security issue was found in Apache Xalan Java XSLT library concerning processing malicious XSLT stylesheets. The copy of Xalan contained in Java runtime is affected as well. The vulnerability was published in National Vulnerability Database (NVD).

1.5 CVE issue(s)

Current description (2022-08-02):

The Apache Xalan Java XSLT library is vulnerable to an integer truncation issue when processing malicious XSLT stylesheets. This can be used to corrupt Java class files generated by the internal XSLTC compiler and execute arbitrary Java bytecode. The Apache Xalan Java project is dormant and in the process of being retired. No future releases of Apache Xalan Java to address this issue are expected. Note: Java runtimes (such as OpenJDK) include repackaged copies of Xalan.

https://nvd.nist.gov/vuln/detail/CVE-2022-34169

1.6 Root Causes

The root cause is located in Xalan XSLT stylesheet processing (integer truncation).

1.7 Resolution

After detection of the issue, possible attack vectors for the components of tts Performance Suite were analyzed. The components have been checked for usages of Xalan XSLT transformation.

Conclusion:

Neither Curator, Webaccess nor QuickAccess are using XSLT transformation. No XSLT files are explicitly processed.

The Producer uses XSLT transformation for export format creation, but employs a different library (Saxon).

Thus, none of the tts Performance Suite components are vulnerable to the attack via Xalan.

1.8 Detection

The issue was detected by tts in the course of the routinely running OWASP dependency check.

1.9 Timeline

2022-07-29

- Detection via OWASP dependency check
- Analyzing the issue and attack vector on tts Performance Suite
- Internal communication

2022-08-02

- Finalizing analysis
- Internal communication

2022-08-04

- External communication

1.10 Supporting information

No actions necessary concerning the tts Performance Suite. We recommend the use of the most current Java implementations.