SSA-632164: External Entity Injection Vulnerability in Polarion ALM

Publication Date: 2023-04-11
Last Update: 2023-05-09
Current Version: V1.1
CVSS v3.1 Base Score: 5.9

SUMMARY

Polarion ALM is vulnerable to XML External Entity (XXE) injection attack that could allow an attacker to potentially disclose confidential data.

Siemens has released an update for Polarion ALM and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Polarion ALM: All versions < V22R2	Update to V22R2 or later version https://support.sw.siemens.com/ See 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:

- Set the below configurations to mitigate against external entity injection in OpenSAML 4.x parser configuration. This will be included by default on Polarion V2304 and later versions.

```
parserPool.setMaxPoolSize(100);

parserPool.setCoalescing(true);

parserPool.setIgnoreComments(true);

parserPool.setIgnoreElementContentWhitespace(true);

parserPool.setNamespaceAware(true);

parserPool.setExpandEntityReferences(false);

parserPool.setXincludeAware(false);

final Map<String, Boolean> features = new HashMap<String, Boolean>();

features.put(http://xml.org/sax/features/external-general-entities, Boolean.FALSE
);

features.put(http://xml.org/sax/features/external-parameter-entities, Boolean.
FALSE);

features.put(http://apache.org/xml/features/disallow-doctype-decl, Boolean.TRUE);

features.put(http://apache.org/xml/features/validation/schema/normalized-value,
Boolean.FALSE);

features.put(http://javax.xml.XMLConstants/feature/secure-processing, Boolean.
TRUE);

parserPool.setBuilderFeatures(features);
```

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

Polarion ALM is an application lifecycle management solution that improves software development processes with a single, unified solution for requirements, coding, testing, and release.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2023-28828

The application contains a XML External Entity Injection (XXE) vulnerability. This could allow an attacker to view files on the application server filesystem.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-611: Improper Restriction of XML External Entity Reference

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Cale Anderson for reporting the vulnerability

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 (2023-04-11): Publication Date
V1.1 (2023-05-09): Corrected fix version to an earlier release of Polarion ALM that fixes the vulnerability; Updated CVSS rating of CVE-2023-28828

TERMS OF USE