SSA-871717: Multiple Vulnerabilities in Polarion ALM

Publication Date: 2024-02-13
Last Update: 2024-05-14
Current Version: V1.2
CVSS v3.1 Base Score: 7.8
CVSS v4.0 Base Score: 8.5

SUMMARY

Polarion ALM is affected by incorrect default path permissions in installation path, and improper authentication in the REST API endpoints of DOORS connector. An attacker could exploit the vulnerabilities for unauthenticated access, or privilege escalation.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Polarion ALM: All versions < V2404.0 affected by all CVEs	Update to V2404.0 or later version https://support.sw.siemens.com/ 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-2023-50236:
  - In Polarion Windows installation, restrict permissions of BUILTIN\Users from accessing the entire Polarion installation folders to prevent data corruption. Please refer to the Additional Information section for further details.
  - Polarion installations in Linux are not impacted. Hence no actions are required.
- CVE-2024-23813:
  - If DOORS connector is not used in the environment, it is advised to limit unauthenticated access within the Apache configuration. For further details, please refer to the Additional Information section.
  - If DOORS connector is used in the environment, restrict access to DOORS connector endpoint to the IP address of the DOORS instance with which Polarion synchronizes its data, which can be done in two ways:
    - Firewall rules set by network administrator (preferred and safest method).
    - Configure Apache using guidelines https://httpd.apache.org/docs/2.4/howto/access.html

    For further details, please refer to the Additional Information section.

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 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-2023-50236

The affected product is vulnerable due to weak file and folder permissions in the installation path. An attacker with local access could exploit this vulnerability to escalate privileges to NT AUTHORITY\SYSTEM.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	8.5
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-276: Incorrect Default Permissions

Vulnerability CVE-2024-23813

The REST API endpoints of doorsconnector of the affected product lacks proper authentication. An unauthenticated attacker could access the endpoints, and potentially execute code.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CVSS v4.0 Base Score	6.9
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:L/SI:N/SA:N
CWE	CWE-287: Improper Authentication

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Michael Heinzl for coordinated disclosure of CVE-2023-50236
- Deniz Cevik from Cyberwise Turkiye for reporting the vulnerability CVE-2024-23813

ADDITIONAL INFORMATION

CVE-2023-50236

In order to restrict file and folder path permissions post installation for the Windows Polarion installation, execute below commands from Windows powershell as administrator. Please note that POLARION_HOME is the path to the folder named “Polarion”, do not confuse it with Polarion/polarion.

- `icacls "<POLARION_HOME>" /grant "BUILTIN\Administrators:(OI)(CI)F" /grant "NT AUTHORITY\SYSTEM:(OI)(CI)F"`
- `icacls "<POLARION_HOME>" /inheritance:r`
- `icacls "<POLARION_HOME>\bundled\postgres" /grant "BUILTIN\Users:(OI)(CI)RX"`

The below command is required by Postgresql installation. It provides read and execution rights on “data” folder only and those rights are not propagated to the subfolders. The “data” folder itself doesn’t contain any file and the contained subfolders will not be accessible by BUILTIN\Users, thus no confidential data can be disclosed. `icacls "<POLARION_HOME>\data" /grant "BUILTIN\Users:RX"`

The below command is optional. It can be used to grant access to BUILTIN\Users to the README.html and README_OSS.html located into the POLARION_HOME. `icacls "<POLARION_HOME>\*.html" /grant "BUILTIN\Users:R"`

CVE-2024-23813

DOOR Connectors are not used: It is recommended to deny unauthenticated access using the below steps:

- Add the following in polarion(-cluster).conf in any Polarion node instance. `<If "%{REQUEST_URI} =~ m#^/polarion/doorsconnector/rest#"> Require all denied </If>`
- Enable the mod_headers in httpd(-cluster).conf by adding `LoadModule headers_module modules/mod_headers.so` after any `LoadModule directives`. If `#LoadModule headers_module modules/mod_headers.so` is present then remove the # to make it effective.
- Restart Apache Http server on every node.

DOOR Connectors are used: It is recommended to restrict the access via Apache configuration. This can be done in two ways by adding the below configuration to polarion(-cluster).conf of every Polarion node.

- To restrict the access based on the hostname, the allowed hostnames must be separated by space. This can be done by using the fully qualified domain name (or a partial domain name). `<If "%{REQUEST_URI} =~ m#^/polarion/doorsconnector/rest#"> Require host myhost.mycompanydomain.com myhostalias.mycompanydomain.com</If>`
- To restrict the access based on the client IP address, the allowed IP addresses must be separated by space. `<If '%{REQUEST_URI} =~ m#^/polarion/doorsconnector/rest#'> Require ip 127.0.0.1 123.123.123.7 </If>`
- Enable the mod_headers in httpd(-cluster).conf by adding `LoadModule headers_module modules/mod_headers.so` after any `LoadModule directives`. If `#LoadModule headers_module modules/mod_headers.so` is present then remove the # to make it effective.
- Restart Apache Http server on every node.

Any request coming from non legit hostnames or IP addresses will produce 403 HTTP Status code.

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 (2024-02-13): Publication Date
V1.1 (2024-03-12): Added additional mitigation measures, with detailed description in Additional Information
V1.2 (2024-05-14): Added fix for Polarion ALM

TERMS OF USE