# SSA-562051: Cross-Site Scripting Vulnerability in Polarion ALM

Publication Date: 2022-03-08
Last Update: 2022-04-12
Current Version: V1.1
CVSS v3.1 Base Score: 6.5

## SUMMARY

The Subversion Webclient in Polarion ALM contains a cross-site scripting vulnerability, that could be triggered by an attacker by sending crafted links to an administrator user of Polarion ALM.

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

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| Polarion ALM:<br>All versions < V21 R2 P2 | Update to V21 R2 P2 or later version<br>https://support.sw.siemens.com/knowledge-base/PL8613685<br>See further recommendations from section Workarounds and Mitigations |
| Polarion WebClient for SVN:<br>All versions | Currently no fix is planned<br>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:

- Do not open links from untrusted sources while working on Polarion Subversion webclient

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.

Polarion WebClient for SVN, one of several free Subversion tools from Polarion Software, is a SVN client that enables Subversion users to work with SVN repositories using a web browser. (https://polarion.plm.automation.siemens.com/products/svn/svn_webclient)

## 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-2021-44478

A cross-site scripting is present due to improper neutralization of data sent to the web page through the SVN WebClient in the affected product.

An attacker could exploit this to execute arbitrary code and extract sensitive information by sending a specially crafted link to users with administrator privileges.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |

## ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Nicolas Briand from Thales Digital Factory for coordinated disclosure

## 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 (2022-03-08): | Publication Date |
| V1.1 (2022-04-12): | Corrected list of affected versions; clarified difference between Polarion ALM and the freeware (WebClient for SVN) |

## TERMS OF USE