SSA-792594: Host Header Injection Vulnerability in Polarion ALM

Publication Date: 2022-12-13
Last Update: 2022-12-13
Current Version: V1.0
CVSS v3.1 Base Score: 5.4

SUMMARY

Polarion ALM contains a misconfiguration in its default Apache HTTP Server configuration that could allow an attacker to perform host header injection attacks.

Siemens is preparing updates and recommends specific countermeasures for existing installations by checking for misconfigurations in configuration files.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Polarion ALM: All versions	Currently no fix is available 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:

- In the product's Apache HTTP Server configuration, check `polarion.conf` or `polarion-cluster.conf` for the below misconfiguration:

  `RedirectMatch permanent ^/$ /polarion/` which must be changed to `RedirectMatch permanent "^/$" "https://<their-polarion-host-here>/polarion/"`

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-2022-46265

The affected application contains a Host header injection vulnerability that could allow an attacker to spoof a Host header information and redirect users to malicious websites.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:T/RC:C
CWE	CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Pongsathon Sirithanyakul, Juttikhun Jirathanan, and Warunyou Sunpachit from IT Select Lab Co.,Ltd. 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 (2022-12-13): Publication Date

TERMS OF USE