SSA-274282: Cross Site Scripting Vulnerability in PLM Help Server V4.2

Publication Date: 2022-12-13
Last Update: 2022-12-13
Current Version: V1.0
CVSS v3.1 Base Score: 6.1

SUMMARY

The Siemens PLM Help Server V4.2 for documentation contains a reflected cross-site scripting vulnerability. This product has reached end of life, and security vulnerabilities are no longer patched.

Siemens has released a new version of Documentation Server that resolves this vulnerability. See the chapter “Additional Information” below for more details.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
PLM Help Server V4.2: All versions	Currently no fix is planned 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 unknown links while working on PLM Help Server V4.2

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

PLM Help Server is a documentation server used for hosting the Help or Manuals files.

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-2022-44575

A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected application that could allow an attacker to execute malicious javascript code by tricking users into accessing a malicious link.

CVSS v3.1 Base Score	6.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:U/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Michael Heinzl for reporting the vulnerability

ADDITIONAL INFORMATION

Siemens recommends to upgrade to Siemens Documentation Server V2.1 or later version. Once the new Documentation Server is installed, you will need to download and install the documentation packages. Information on this is included in the install guides. Refer to PL8681100 for 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