SSA-436520: XSS and CSRF Vulnerabilities in Polarion Subversion Webclient

Publication Date: 2020-09-08
Last Update: 2020-09-08
Current Version: V1.0
CVSS v3.1 Base Score: 8.1

SUMMARY

Multiple cross-site scripting (XSS) vulnerabilities were found in the subversion webclient of Polarion. In addition, the webclient doesn't have any cross-site request forgery (CSRF) protection. An attacker could inject client side script to induce the victim to issue an HTTP request that would lead to a state changing operation. Siemens recommends specific countermeasures as there are currently no fixes available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Polarion Subversion Webclient: All versions	The tool is considered shareware, distributed "as is" and there will not be a fix as it is no longer supported

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 Polarion Subversion webclient

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 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.

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-2020-15788

The Polarion subversion web application does not filter user input in a way that prevents Cross-Site Scripting.

If a user is enticed into passing specially crafted, malicious input to the web client (e.g. by clicking on a malicious URL with embedded JavaScript), then JavaScript code can be returned and may then be executed by the user's client.

Various actions could be triggered by running malicious JavaScript code.

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-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

Vulnerability CVE-2020-15789

The web interface could allow a Cross-Site Request Forgery (CSRF) attack if an unsuspecting user is tricked into accessing a malicious link.

Successful exploitation requires user interaction by a legitimate user, who must be authenticated to the web interface. A successful attack could allow an attacker to trigger actions via the web interface that the legitimate user is allowed to perform. This could allow the attacker to read or modify contents of the web application.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:U/RC:C
CWE	CWE-352: Cross-Site Request Forgery (CSRF)

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Li Yifan from Bolean Technology LTD. 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 (2020-09-08): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through

a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.