SSA-938930: Cross-Site Scripting Vulnerability in Spectrum Power™ 5

Publication Date:	2020-03-10
Last Update:	2020-03-10
Current Version:	V1.0
CVSS v3.1 Base Score:	6.1

SUMMARY

A Cross-Site Scripting (XSS) vulnerability was found in the Engineering User Interface of Spectrum Power™ 5.

A software update is available to address the issue and Siemens recommends installing the patch.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Spectrum Power™ 5: All versions < v5.50 HF02	Please contact Siemens Energy Customer Support Center at: support.energy@siemens.com or your local Siemens representative.

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 Spectrum Power™ 5.

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs or DSOs) worldwide are usually required by regulations to build resilience into the power grids by applying multi-level redundant secondary protection schemes. It is therefore recommended that the operators check whether appropriate resilient protection measures are in place. The risk of cyber incidents impacting the grid's reliability can thus be minimized by virtue of the grid design.

Siemens strongly recommends applying the provided security updates using the corresponding tooling and documented procedures made available with the product. If supported by the product, an automated means to apply the security updates across multiple product instances may be used. Siemens strongly recommends prior validation of any security update before being applied, and supervision by trained staff of the update process in the target environment.

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

Recommended security guidelines to Digital Grid Products can be found at:

https://www.siemens.com/gridsecurity

PRODUCT DESCRIPTION

Spectrum Power™ 5 is used for the automation of power supply networks in industry and for gas, water, district heating, and power supply grids operated by public utilities.

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-2020-7579

The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link.

User interaction is required for a successful exploitation.

If deployed according to recommended system configuration, Siemens considers the environmental vector as CR:L/IR:M/AR:H/MAV:A (4.1).

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:O/RC:C
CWE	CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Kudelski Security Pentesting Team 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 (2020-03-10):	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.