SSA-747162: Cross-Site Scripting Vulnerability in Spectrum Power™

Publication Date: 2019-07-09
Last Update: 2019-08-13
Current Version: V1.1
CVSS v3.0 Base Score: 4.7

SUMMARY

A Cross-Site Scripting (XSS) vulnerability was found in the WebSDK component of Spectrum Power™ 3, 4, 5 and 7.

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 3 (Corporate User Interface): All versions <= v3.11	Please contact Siemens Energy Customer Support Center at: support.energy@siemens.com or your local Siemens representative.
Spectrum Power 4 (Corporate User Interface): Version v4.75	Please contact Siemens Energy Customer Support Center at: support.energy@siemens.com or your local Siemens representative.
Spectrum Power 5 (Corporate User Interface): All versions < v5.50	Please contact Siemens Energy Customer Support Center at: support.energy@siemens.com or your local Siemens representative.
Spectrum Power 7 (Corporate User Interface): All versions <= v2.20	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 allow Internet access for Spectrum Power UI clients.
- Users should be trained to avoid clicking on unknown links.

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs) 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 Secure Substations can be found at:

https://www.siemens.com/gridsecurity

PRODUCT DESCRIPTION

Spectrum Power™ 3 SCADA applications provide functions required for monitoring, alarming, measuring, calculating, archiving and safe supervisory control based on analog and digital measurements, accumulator values, and momentaries.

Spectrum Power™ 4 provides basic components for SCADA, communications, and data modeling for control and monitoring systems. Application suites can be added to optimize network and generation management for all areas of energy management.

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.

Spectrum Power™ 7 was developed for energy management in power transmission and distribution systems as well as for controlling railway power supply systems.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2019-10933

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. The user does not need to be logged into the web interface in order for the exploitation to succeed.

At the stage of publishing this security advisory no public exploitation is known.

CVSS v3.0 Base Score	4.7
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- İsmail Mert AY AK from Biznet Bilişim A.Ş. for coordinated disclosure
- CISA-Industrial Control System Vulnerability Disclosure team for coordination efforts

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 (2019-07-09): Publication Date
V1.1 (2019-08-13): Corrected version information for Spectrum Power 5

TERMS OF USE