

## **SSA-568969: Insecure Storage of Sensitive Information in Spectrum Power™ 4**

Publication Date: 2020-09-08  
Last Update: 2020-09-08  
Current Version: V1.0  
CVSS v3.1 Base Score: 3.7

### **SUMMARY**

Vulnerabilities in Spectrum Power™ 4 could allow an unauthorized attacker to retrieve a list of software users, or in certain cases to list the contents of a directory.

Siemens has released updates and configuration recommendations for Spectrum Power™ 4 in order to mitigate the issues.

### **AFFECTED PRODUCTS AND SOLUTION**

Affected Product and Versions	Remediation
Spectrum Power™ 4: All versions < V4.70 SP8	Please contact your local Siemens representative.

### **WORKAROUNDS AND MITIGATIONS**

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Siemens offers mitigations for customers. Please contact your local Siemens representative for further information.

### **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™ 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.

## **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-2020-15784

Insecure storage of sensitive information in the configuration files could allow the retrieval of user names.

CVSS v3.1 Base Score	3.7
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C</a>
CWE	CWE-312: Cleartext Storage of Sensitive Information

### Vulnerability CVE-2020-15790

If configured in an insecure manner, the web server might be susceptible to a directory listing attack.

CVSS v3.1 Base Score	3.7
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C</a>
CWE	CWE-548: Exposure of Information Through Directory Listing

## **ACKNOWLEDGMENTS**

Siemens thanks the following parties for their efforts:

- Can Demirel from Cyberwise 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](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.