SSA-324467: OS Command Injection in Spectrum Power 4.7

Publication Date: 2019-04-09
Last Update: 2019-04-09
Current Version: V1.0
CVSS v3.0 Base Score: 10.0

SUMMARY

Versions of Spectrum Power™ 4, that use the customer specific project enhancement (PE) Web Office Portal (WOP) are affected by a possible OS Command Injection vulnerability. Siemens has released patches for the affected version and recommends to apply specific countermeasures until these patches can be applied.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Spectrum Power™ 4: with Web Office Portal	Take over bugfix bf-47456_PE_WOP_fix. Bugfix bf-47456_PE_WOP_fix for Web Office Portal can be obtained from the Siemens Energy Customer Support Center at: support.energy@siemens.com

WORKAROUNDS AND MITIGATIONS

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

- Turn off the web server or limit access to the web server by an external firewall.

GENERAL SECURITY RECOMMENDATIONS

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™ 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 3.0 (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-2019-6579

An attacker with network access to the web server on port 80/TCP or 443/TCP could execute system commands with administrative privileges.

The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected service. No user interaction is required to exploit this security vulnerability. Successful exploitation of the security vulnerability compromises confidentiality, integrity or availability of the targeted system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	10.0
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Applied Risk 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 (2019-04-09): Publication Date

TERMS OF USE