SSA-545214: Vulnerability in ViewPort for Web Office Portal

Publication Date 2017-06-29
Last Update 2017-06-29
Current Version V1.0
CVSS v3.0 Base Score 9.8

SUMMARY

The latest update for ViewPort for Web Office Portal fixes a vulnerability that could allow unauthenticated remote users to perform code execution under certain conditions.

AFFECTED PRODUCTS

- ViewPort for Web Office Portal: All versions < Revision number 1453

DESCRIPTION

The Web Office Portal provides authorized users to retrieve the current data from the control center solution Spectrum Power™ in a read only manner without direct access to the control center solution itself, display it by means of established programs of the office world and eventually process the data as needed.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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 assessed by the customer to accomplish final scoring.

Vulnerability Description (CVE-2017-6869)

An unauthenticated remote user could upload arbitrary code and execute it with the permissions of the operating system user running the web server by sending specially crafted network packets to port 443/TCP or port 80/TCP.

CVSS Base Score 9.8
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Mitigating Factors

The attacker must have network access to the web server on port 443/TCP or port 80/TCP of the affected product. Siemens recommends operating the affected product only within trusted networks [3].

SOLUTION

Siemens provides software revision number 1453 for ViewPort for Web Office Portal which fixes the vulnerability and supports customers to update to the fixed version.

Siemens recommends the following mitigations until patches can be applied:

- Protect access to port 443/TCP and port 80/TCP of the affected product with appropriate measures
- Disable port 80/TCP and use TLS client certificates (PKI) to access port 443/TCP
- Apply Defense-in-Depth [2]

ACKNOWLEDGEMENTS

Siemens thanks Hannes Trunde from Kapsch BusinessCom AG for coordinated disclosure.

ADDITIONAL RESOURCES

[1] Revision number 1453 for ViewPort for Web Office Portal can be obtained from the Siemens Energy Customer Support Center at: support.energy@siemens.com

[2] Information about Grid Security by Siemens: https://www.siemens.com/gridsecurity

[3] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT: https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2017-06-29): Publication Date

DISCLAIMER