SSA-563539: Vulnerabilities in OZW672 and OZW772

Publication Date 2017-07-04
Last Update 2017-07-04
Current Version V1.0
CVSS v3.0 Base Score 7.4

SUMMARY

OZW672 and OZW772 devices are affected by two vulnerabilities, which could allow attackers to read and write historical measurement data under certain conditions, or to read and modify data in TLS sessions.

Siemens recommends customers to apply specific mitigations.

AFFECTED PRODUCTS

- OZW672: All versions
- OZW772: All versions

DESCRIPTION

OZW devices are used for remote monitoring of building controller devices, e.g. for monitoring of heating control or of air conditioning systems.

Detailed information about the vulnerabilities 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 1 (CVE-2017-6872)

An attacker with access to port 21/tcp could access or alter historical measurement data stored on the device.

CVSS Base Score 6.5
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:T/RC:C

Vulnerability 2 (CVE-2017-6873)

A vulnerability in the integrated web server on port 443/tcp could allow an attacker to read and manipulate data in TLS sessions while performing a man-in-the-middle (MITM) attack.

CVSS Base Score 7.4
CVSS Vector CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:T/RC:C

SOLUTION

Siemens recommends applying the following mitigations:

- Protect network access to the affected devices
- Disable integrated service on port 21/tcp in the device settings by changing the value of “ACS access” under “Settings > Communication > Services to “Off”. Applying this configuration change mitigates Vulnerability 1 entirely

- Use the web portal as described in the product documentation for all applications; Connections to the web portal are not affected by Vulnerability 2
- If use of web portal is not possible, then use the integrated web server only in trusted networks

ACKNOWLEDGEMENTS

Siemens thanks Stefan Viehböck from SEC Consult for coordinated disclosure of the vulnerabilities.

ADDITIONAL RESOURCES

[1] 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 (2017-07-04): Publication Date

DISCLAIMER