# SSA-945660: Privilege Enforcement Vulnerability in XHQ

Publication Date 2017-06-22
Last Update 2017-06-22
Current Version V1.0
CVSS v3.0 Base Score 6.5

## SUMMARY

The latest updates for XHQ 4 and XHQ 5 fix a vulnerability that could allow a low-privileged remote user to gain read access to data in the XHQ solution exceeding his configured permission level.

## AFFECTED PRODUCTS

- XHQ 4: All versions < V4.7.1.3
- XHQ 5: All versions < V5.0.0.2

## DESCRIPTION

XHQ Operations Intelligence product line aggregates, relates and presents operational and business data in real-time to improve enterprise performance. Through XHQ, you have a single coherent view of information, enabling a variety of solutions in real-time performance management and decision support.

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-2017-6866)

A vulnerability in XHQ server could allow an authenticated low-privileged remote user to gain read access to data in the XHQ solution exceeding his configured permission level.

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

## SOLUTION

Siemens provides XHQ V4.7.1.3 [1] and XHQ V5.0.0.2 [1] which fix the vulnerability and recommends customers to update to the new version.

As a general security measure Siemens strongly recommends to protect network access to XHQ with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [2] in order to run the devices in a protected IT environment.

## ADDITIONAL RESOURCES

[1] Please call your local service organization for further information on how to obtain the new version of XHQ. If assistance in identifying your local service organization is required, please call a local Siemens hotline center:
https://w3.siemens.com/aspa_app/

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

  

[3] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[4] 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 (2017-06-22): Publication Date

## DISCLAIMER