

## **SSA-712690: Vulnerabilities in XHQ Operations Intelligence**

Publication Date: 2020-12-08  
Last Update: 2020-12-08  
Current Version: V1.0  
CVSS v3.1 Base Score: 8.1

### **SUMMARY**

Multiple vulnerabilities have been identified in the XHQ Operations Intelligence product line. These vulnerabilities could allow for data injection in the XHQ's web interfaces.

Siemens recommends to update XHQ Operations Intelligence product line to the newest version.

### **AFFECTED PRODUCTS AND SOLUTION**

<b>Affected Product and Versions</b>	<b>Remediation</b>
XHQ: All Versions < 6.1	Update to V6.1 or later, or apply recommendations from section Workarounds and Mitigations 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: <a href="https://w3.siemens.com/aspa_app/">https://w3.siemens.com/aspa_app/</a>

### **WORKAROUNDS AND MITIGATIONS**

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

- Follow XHQ's documentation on how to implement a secure configuration for IIS

### **GENERAL SECURITY RECOMMENDATIONS**

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: <https://www.siemens.com/cert/operational-guidelines-industrial-security>), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: <https://www.siemens.com/industrialsecurity>

### **PRODUCT 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.

### **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-2019-19283

The application's web server could expose non-sensitive information about the server's architecture. This could allow an attacker to adapt further attacks to the version in place.

CVSS v3.1 Base Score	5.3
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C</a>
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

#### Vulnerability CVE-2019-19284

The web interface could allow Cross-Site Scripting (XSS) attacks if an attacker is able to modify content of particular web pages, causing the application to behave in unexpected ways for legitimate users.

CVSS v3.1 Base Score	6.3
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C</a>
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

#### Vulnerability CVE-2019-19285

The web interface could allow injections that could lead to XSS attacks if unsuspecting users are tricked into accessing a malicious link.

CVSS v3.1 Base Score	6.3
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C</a>
CWE	CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

#### Vulnerability CVE-2019-19286

The web interface could allow SQL injection attacks if an attacker is able to modify content of particular web pages.

CVSS v3.1 Base Score	7.2
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C</a>
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

#### Vulnerability CVE-2019-19287

The web interface could allow attackers to traverse through the file system of the server based by sending specially crafted packets over the network without authentication.

CVSS v3.1 Base Score	6.5
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C</a>
CWE	CWE-23: Relative Path Traversal

### Vulnerability CVE-2019-19288

The web interface could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

### Vulnerability CVE-2019-19289

The web interface could allow a Cross-Site Request Forgery (CSRF) attack if an unsuspecting user is tricked into accessing a malicious link.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-352: Cross-Site Request Forgery (CSRF)

## **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 (2020-12-08): 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.