SSA-525454: Vulnerabilities in XHQ Operations Intelligence

Publication Date: 2019-12-10
Last Update: 2019-12-10
Current Version: V1.0
CVSS v3.1 Base Score: 8.8

SUMMARY

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

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
XHQ: All versions < V6.0.0.2	Update to V6.0.0.2 or later 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/

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.
- Allow communications to XHQ only by HTTPS.

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-2019-13930

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

Successful exploitation requires user interaction by a legitimate user, who must be authenticated to the web interface. A successful attack could allow an attacker to trigger actions via the web interface that the legitimate user is allowed to perform. This could allow the attacker to read or modify contents of the web application.

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

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)

Vulnerability CVE-2019-13931

The web interface could allow for an an attacker to craft the input in a form that is not expected, causing the application to behave in unexpected ways for legitimate users.

Successful exploitation requires for an attacker to be authenticated to the web interface. A successful attack could cause the application to have unexpected behavior. This could allow the attacker to modify contents of the web application.

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

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

Vulnerability CVE-2019-13932

The web application requests could be manipulated, causing the the application to behave in unexpected ways for legitimate users.

Successful exploitation does not require for an attacker to be authenticated. A successful attack could allow the import of scripts or generation of malicious links. This could allow the attacker to read or modify contents of the web application.

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

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

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 (2019-12-10): 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, 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.