ABB DOC ID: 9AKK107492A9962
REVISION: B
DATE: 2020-02-17

CYBER SECURITY ADVISORY

Asset Suite Direct Object Reference Vulnerability

ABBVU-PGGA-2019013

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Affected Products

Asset Suite versions 9.0.0 to 9.6.0, not including 9.4.2.6 and 9.5.3.2

Vulnerability ID

ABB ID: ABBVU-PGGA-2019013

Summary

An update is available that resolves a privately reported vulnerability in the product versions listed above.

An attacker who successfully exploited this vulnerability could gain access to unauthorized information in the application by accessing resources directly.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVSS v3 Base Score:	7.1
CVSS v3 Temporal Score:	6.4
CVSS v3 Vector:	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C:
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C
CVEID:	CVE-2019-18998

Recommended immediate actions

The vulnerability is corrected in the following product versions:

Asset Suite 9.4.2.6

Asset Suite 9.5.3.2

Asset Suite 9.6.1

ABB recommends that customers apply the update as soon as they are able.

Vulnerability Details

A Direct Object Reference vulnerability exists in the web interface included with Asset Suite versions 9.0.0 to 9.6.0, not including 9.4.2.6 and 9.5.3.2. There is a flaw in the access controls used to limit user access to resources. If an attacker knows, or were to discover, the URL for a resource they do not have permissions to, they would be able to access the resource by browsing directly to the URL.

Mitigating Factors

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

Workarounds

No workarounds exist at this time.

Frequently Asked Questions

What causes the vulnerability?

The vulnerability is caused by a lack of proper access control checks when accessing resources within the application.

What is the affected product or component?

Asset Suite versions 9.0.0 to 9.6.0, not including 9.4.2.6 and 9.5.3.2

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability would be able to gain access to unauthorized resources affecting the confidentiality and integrity of information.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by browsing directly to an objects location instead of going through the menu. A user that knows the direct URL can enter that into the browser address bar and gain access to the resource.

Could the vulnerability be exploited remotely?

An attacker who has network access to the application web interface and has valid authentication credentials would be able to exploit this vulnerability.

What does the update do?

The update removes the vulnerability by implementing the authorization logic in the administrative pages/workflows. Asset Suite now throws “User Not Authorized” exception when the user tries to access the administrative workflow pages using their direct URLs unless he/she has necessary roles (Asset Suite security profiles).

Asset Suite panel mode pages already implement authorization checks.

When this security advisory was issued, had this vulnerability been publicly disclosed?

No, ABB received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally.

Acknowledgements

None.

Support

For additional information and support please contact your local ABB service organization. For contact information, see https://new.abb.com/contact-centers.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.