ABB DOC ID: 3CCA2020-003309
REVISION: A
DATE: 2022-09-19

CYBER SECURITY ADVISORY

SECURITY ABB Central Licensing System Vulnerabilities, impact on ABB Ability™ SCADAvantage

CVE ID: CVE-2020-8475, CVE-2020-8476, CVE-2020-8479

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.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected Products

ABB Central Licensing System (CLS) as used in ABB Ability™ SCADAvantage versions 5.1 to 5.6.5.

Summary

This document is a complement to the generic ABB Cyber Security Advisory "Multiple Vulnerabilities in ABB Central Licensing System" (2PAA121231) which is available under https://new.abb.com/about/technology/cyber-security ➔ Alerts and Notifications.

This document provides additional information specific to ABB Ability™ SCADAvantage as it utilizes versions of the ABB Central Licensing System (CLS) that are affected by vulnerabilities. The table indicates for ABB Ability™ SCADAvantage versions 5.1 to 5.6.5 which of the two installation types of CLS - Client-Server and Standalone, both possible with ABB Ability™ SCADAvantage - are affected and by which vulnerabilities.

CVE ID	Vulnerability	ABB Ability™ SCADAvantage 5.1 to 5.6.5	
		CLS Client-Server Installation	CLS Standalone Installation
CVE-2020-8475	Denial of Service	Affected	Not Affected
CVE-2020-8476	Elevation of privilege vulnerability	Affected	Not Affected
CVE-2020-8479	XML External Entity Injection vulnerability	Affected	Not Affected

Vulnerability Details

ABB is aware that the Central Licensing System, which is used by ABB Ability™ SCADAvantage contains several vulnerabilities which require user attention:

1. **CVE-2020-8475:** Denial of Service vulnerability: An attacker who successfully exploited this vulnerability could cause the license service to fail.
2. **CVE-2020-8476:** Elevation of privilege vulnerability: An attacker who successfully exploited this vulnerability in the license server could alter licenses assigned to the system nodes. This could potentially lead to a situation where legitimate nodes in the system network are denied licenses.
3. **CVE-2020-8479:** XML External Entity Injection vulnerability: An attacker who successfully exploited the vulnerabilities could read or call arbitrary files from the license server and/or from the network and may also block the license handling.

Exploitation of some of these vulnerabilities may block the license handling service, however, the ABB Ability™ SCADAvantage program will continue to operate normally. In some cases, additionally an annoyance messages may be displayed on the user interfaces.

Affected product versions in detail

The following table lists the CLS versions and the associated ABB Ability™ SCADAvantage versions and indicates which of the vulnerabilities these are affected by.

Only the Client-Server installation of CLS is affected as listed in the table below, the Standalone installation is not affected by any of the listed vulnerabilities.

SCADAvantage version	CLS version (Client-Server)	CVE-2020-8475	CVE-2020-8476	CVE-2020-8479	CVE-2020-8481	CVE-2020-8471
5.1	5.1.0-6 (5.1.0.100)	Y	Y	Y	N	N
5.2	5.1.0-6 (5.1.0.100)	Y	Y	Y	N	N
5.3.X	5.1.0-6 (5.1.0.100)	Y	Y	Y	N	N
5.4.X	5.1.0-6 (5.1.0.100)	Y	Y	Y	N	N
5.5.X	5.1.0-6 (5.1.0.100)	Y	Y	Y	N	N
5.6.X	6.0.0-0 (6.0.0.26)	Y	Y	Y	N	N
5.6.5 May 2022 patch	6.1.1-0 (6.1.01100.539)	N	N	N	N	N

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.

CVE-2020-8475 – ABB CLS – Denial of Service

CVSS v3.0 Base Score:	5.3 (Medium)
CVSS v3.0 Temporal Score:	4.9 (Medium)
CVSS v3.0 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:W/RC:C
CVSS v3.0 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:W/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-8475

CVE-2020-8476 – ABB CLS – Elevation of privilege vulnerability

CVSS v3.0 Base Score:	5.3 (Medium)
CVSS v3.0 Temporal Score:	4.9 (Medium)
CVSS v3.0 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:W/RC:C
CVSSv3.0 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:W/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-8476

CVE-2020-8479 - ABB CLS - XXE vulnerability

CVSSv3.0Base Score:	9.3 (High)
CVSSv3.0Temporal Score:	8.4 (High)
CVSS v3.0 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L/E:P/RL:O/RC:C
CVSS v3.0 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L/E:P/RL:O/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-8479

Recommended immediate actions

It is recommended to upgrade to the latest version of ABB Ability™ SCADAvantage version 5.6.5 with ABB Central License Server version 6.1.1-0 (6.1.01000.502), which resolves the **CVE-2020-8475**, **CVE-2020-8476**, and **CVE-2020-8479** vulnerability.

Also, validate that the security practices and firewall configurations are adhering to common practices, in order to protect a network and its attached devices from attacks that originate from outside the network. For example, common practices are for SCADA servers to be physically protected from direct access by un-authorized 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 must be evaluated case by case. SCADA servers and clients should not be used for general business functions (e.g., internet

browsing, email, etc.) which are not critical industrial processes. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a SCADA network.

Mitigating Factors

For CVE-2020-8479, CVE-2020-8475, and CVE-2020-8476 a mitigating factor is that the attacker needs network access to the system network, so an important mitigation is to follow the ABB Ability™ SCADAvantage Cyber Security Guide recommendations and ensure that the SCADA network is protected from unauthorized access. Methods for preventing unauthorized access to nodes on the Client Server Network include but are not limited to usage of IPSec and by separating the SCADA Network from other networks with firewalls.

Workarounds

None.

Acknowledgements

ABB thanks William Knowles and his colleagues at Applied Risk for helping to identify the vulnerabilities and protecting our customers.

Support

For additional information and support please contact your local ABB service organization (contact information, see https://new.abb.com/contact-centers) or ABB Ability™ SCADAvantage support via email SCADAvantagesupport@ca.abb.com

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

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	2022-09-19