DOCUMENT ID: 2PAA121231
REVISION: B
DATE: 2020-04-21

CYBERSECURITY ADVISORY

SECURITY Multiple Vulnerabilities in ABB Central Licensing System

CVE ID: CVE-2020-8481, CVE-2020-8479, CVE-2020-8475, CVE-2020-8476, CVE-2020-8471

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/components

ABB Central Licensing System (CLS) version 5.1 and later.

ABB CLS is not a standalone product but a common component that is exclusively distributed as part of other ABB products. The following table lists all products that are using these versions of CLS and distribute CLS as part of their installation media.

Products	Affected Versions
ABB Ability™ System 800xA and related system extensions	5.1, 6.0 and 6.1
Compact HMI	5.1, 6.0
Control Builder Safe	1.0, 1.1 and 2.0
ABB Ability™ Symphony® Plus - S+ Operations ABB Ability™ Symphony® Plus - S+ Engineering	3.0 to 3.2 1.1 to 2.2
Composer Harmony	5.1, 6.0, 6.1
Composer Melody	Melody Composer 5.3 Melody Composer 6.1 /6.2 SPE for Melody 1.0 SPx (Composer 6.3)
Harmony OPC Server (HAOPC) Standalone	6.0, 6.1, 7.0
ABB Ability™ System 800xA / Advant® OCS Control Builder A Advant® OCS AC 100 OPC Server	1.3 and 1.4 5.1, 6.0 and 6.1
Composer CTK	CTK 6.1, 6.2
AdvaBuild OPC Server for MOD 300 (non-800xA) OPC Data Link	3.7 SP1, 3.7 SP2 1.4 2.1, 2.2
ABB Ability™ Knowledge Manager	8.0, 9.0, 9.1
ABB Ability™ Manufacturing Operations Management	1812 and 1909

Summary

ABB is aware that the ABB Central Licensing System contains several vulnerabilities which require user attention. The above-mentioned products use CLS and are affected by the following vulnerabilities. The table indicates which of the two installation types of CLS that are affected: Client-Server and Standalone.

CVE ID	CVSS * V3 base score	Vulnerability	CLS Client-Server installation	CLS Standalone installation
CVE-2020-8481	9.8	Information Disclosure	Affected	Affected
CVE-2020-8479	9.3	XML External Entity Injection	Affected	Not Affected
CVE-2020-8475	5.3	Denial of Service	Affected	Not Affected
CVE-2020-8476	5.3	Elevation of Privilege	Affected	Not Affected
CVE-2020-8471	7.8	Weak File Permissions	Affected	Affected

* CVSS - Common Vulnerability Scoring System

For some of the affected products the CVSS score may be lower. This is described in the advisories listed in the section “Product specific cybersecurity advisories” below.

Affected CLS versions

This table indicates which CLS versions that are affected. The product specific cybersecurity advisories describe which CLS versions that are used by these products.

ABB Central Licensing System version	CVE-2020-8481	CVE-2020-8479	CVE-2020-8475	CVE-2020-8476	CVE-2020-8471
5.1.0/0 (5.1.0.14) 5.1.0/1 (5.1.0.35)	Y	Y	Y	Y	Y
5.1.0/1 (5.1.0.38) 5.1.0-2 (5.1.0.53) 5.1.0-2 (5.1.0.55) 5.1.0-3 (5.1.0.65) 5.1.0-4 (5.1.0.70) 5.1.0-5 (5.1.0.84)	N	Y	Y	Y	Y
5.1.0-6 (5.1.0.99) 5.1.0-6 (5.1.0.100) 5.1.0-6 (5.1.0.102) 5.1.0-6 (5.1.0.103)	N	Y	Y	Y	N
6.0.0-0 (6.0.0.26) 6.0.1-0 (6.0.00100.54) 6.0.1-0 (6.0.00100.55) 6.0.1-0 (6.0.00100.57) 6.0.3-0 (6.0.03000.73) 6.0.3-0 (6.0.03000.74) 6.0.3-0 (6.0.03000.84) 6.0.3-0 (6.0.03000.95)	N	Y	Y	Y	N
6.0.3-0 (6.0.03000.192)	N	N	Y	Y	N
6.1.0-0 (6.1.00000.16) 6.1.0-0 (6.1.00000.18) 6.1.0-0 (6.1.00000.398)	N	Y	Y	Y	N
6.1.0-0 (6.1.00100.417)	N	N	Y	Y	N

Recommended immediate actions

The product specific cybersecurity advisories provide specific recommendations for the affected products.

Additional general recommendations:
Recommended baseline security practices and firewall configurations can help protect a network and its attached devices from attacks that originate from outside the network. For example, common practices are for process control systems to be 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 must be evaluated case by case. Process control and automation systems 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 control system.

Install software security updates validated by ABB.

Install the updated virus definition files for the recommended / supported malware protection solution.

Vulnerability details

1. **CVE-2020-8481**: Information Disclosure vulnerability: Confidential data is written in an unprotected file. An attacker who successfully exploited this vulnerability could take full control of the computer.
2. **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.
3. **CVE-2020-8475**: Denial of Service vulnerability: An attacker who successfully exploited this vulnerability could block the license handling.
4. **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.
5. **CVE-2020-8471**: Weak File Permissions: An authenticated attacker who successfully exploited this vulnerability, could block the license handling, escalate his/her privileges and execute arbitrary code.

Exploitation of some of these vulnerabilities may block the license handling. The effect of this may differ for different products. A usual behavior is that launching of engineering functions may be blocked and that operator functions may still work but annoyance messages may be displayed. The product specific cybersecurity advisories may describe the behavior in more detail.

Product specific cybersecurity advisories

This section will be updated with references when relevant. The following product specific advisories are available:

– SECURITY ABB Central Licensing System Vulnerabilities, impact on System 800xA, Compact HMI and Control Builder Safe (2PAA121230), http://search.abb.com/library/Download.aspx?DocumentID=2PAA121230&LanguageCode=en&DocumentPartId=&Action=Launch

The following advisory is in preparation, soon to be ready

– SECURITY ABB Central Licensing System Vulnerabilities, impact on Symphony® Plus, Composer Harmony, Composer Melody, Harmony OPC Server

Advisories are being prepared also for the other affected products.

These documents are available at https://new.abb.com/about/technology/cyber-security/alerts-and-notifications. They are also available for registered users, together with more relevant information, in the ABB customer portal (MyABB) in the My Control System section.

Frequently asked questions

What is the scope of the vulnerabilities?

An attacker who successfully exploited these vulnerabilities could take control of the affected system node, remotely cause an affected CLS Server node to stop or prevent legitimate access to the affected CLS Server.

What causes the vulnerabilities?

The vulnerabilities are caused

– by SW writing excessive confidential information into an unprotected file

– by insufficient input data validation in the license server communication.

– by insufficient access control in a folder with executable code.

What is the Central Licensing Service?

The Central Licensing Service actively monitors and enforces the licensed features with the purpose to validate the usage against the licenses that were procured. The CLS server dynamically distributes the available licenses, as required on all other nodes (License Clients) within the system. The user is informed about the possible license violations by means of license violation annoyance popup message.

What might an attacker use the vulnerabilities to do?

See “Vulnerability details” above.

How could an attacker exploit the vulnerabilities?

CVE-2020-8481: ABB CLS - Information Disclosure
An attacker could exploit the vulnerability by logging into the affected node as a low privileged user, read confidential data from an unprotected file.

CVE-2020-8479: ABB CLS - XXE vulnerability
CVE-2020-8475: ABB CLS - Denial of Service vulnerability
CVE-2020-8476: ABB CLS - Elevation of privilege vulnerability
An attacker could exploit these vulnerabilities by sending specially crafted message to the CLS Web Service. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software.

CVE-2020-8471: ABB CLS – Weak File Permissions
An attacker could exploit the vulnerability by logging in to an 800xA node and modify the files in the folders with weak access control lists.

Could the vulnerability be exploited remotely?

CVE-2020-8481: ABB CLS - Information Disclosure
CVE-2020-8471: ABB CLS – Weak File Permissions
No, to exploit this vulnerability an attacker would need to have physical access to an affected system node.

CVE-2020-8479: ABB CLS - XXE vulnerability
CVE-2020-8475: ABB CLS - Denial of Service vulnerability
CVE-2020-8476: ABB CLS - Elevation of privilege vulnerability
Yes, an attacker who has network access to an affected system node could exploit these vulnerabilities remotely. Recommended practices include that process control systems are physically protected, 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.

What do the updates do?

Some of the vulnerabilities have been corrected. Details are described in the advisories listed in the section “Product specific cybersecurity advisories” above.

CVE-2020-8481: ABB CLS - Information Disclosure
The update prevents sensitive information from being written to an unprotected file.

CVE-2020-8479: ABB CLS - XXE vulnerability
The update disables the XML processor from resolving external entities within the DTD.

CVE-2020-8471: ABB CLS – Weak File Permissions
The updates remove the vulnerability by ensuring that the access control list for the folders, limits access to files and folders.

CVE-2020-8475: ABB CLS - Denial of Service vulnerability
CVE-2020-8476: ABB CLS - Elevation of privilege vulnerability
Corrections for these vulnerabilities will be prepared for usage with the different products.

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

No, ABB received information about these vulnerabilities through responsible disclosure.

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

No, ABB had not received any information indicating that these vulnerabilities have been exploited when this security advisory was originally issued.

Acknowledgement

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

Support

For additional instructions and support please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

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

Revisions

Rev.	Page (P) Chapt. (C)	Description	Date
A	all	New document	2020-03-30
B	P2,P4	Revised Vulnerability details and CVSS score for CVE-2020-8479	2020-04-21