DOCUMENT ID: 2PAA121230
REVISION: C
DATE: 2021-07-01

CYBERSECURITY ADVISORY

SECURITY ABB Central Licensing System Vulnerabilities, impact on System 800xA, Compact HMI and Control Builder Safe

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

ABB Central Licensing System (CLS) as used in System 800xA versions 5.1, 6.0 and 6.1

ABB Central Licensing System (CLS) as used in Compact HMI versions 5.1 and 6.0

ABB Central Licensing System (CLS) as used in Control Builder Safe versions 1.0, 1.1 and 2.0.

For more details on which of the vulnerabilities that affect which versions of these products, see section Affected product versions in detail below.

Scope of this document

This document is a complement to the generic ABB Cyber Security Advisory "Multiple Vulnerabilities in ABB Central Licensing System" (2PAA121231) which is available under www.abb.com/cybersecurity → Alerts and Notifications.

This document provides additional information specific to System 800xA, Compact HMI and Control Builder Safe.

Vulnerability IDs and Product Issue Numbers

CVE ID	Product Issue Number*
CVE-2020-8481	800xASRV-IN-5100-001
CVE-2020-8479	800xASRV-OL-5100-011
CVE-2020-8475	800xASRV-OL-5100-012
CVE-2020-8476	800xASRV-OL-5100-013
CVE-2020-8471	800xASRV-OL-5100-014

* Product Issue Number - is an ABB internal unique identifier to identify an issue. The Product Issue Number is for example used to identify the correction of a problem in a Release Note.

Vulnerability details

ABB is aware that the common Central Licensing System used with System 800xA, Compact HMI and Control Builder Safe contains several vulnerabilities which require user attention:

1. **CVE-2020-8481**: Information Disclosure vulnerability: Confidential data is written in an unprotected file. An authenticated attacker who successfully exploited this vulnerability could take full control of the computer. Alternatively CVE-2020-8479 below could be used to read the file via the network and, as seen in the table in "Affected product versions in detail" below, product versions affected by CVE-2020-8481 are also affected by with CVE-2020-8479. This gives CVE-2020-8481 an extra high severity.
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. In System 800xA the effect of this may differ for different products. Launching of engineering functions may be blocked. Operator functions may still work but annoyance messages may be displayed.

Can functional safety be affected by an exploit of any of these vulnerabilities?

CVE-2020-8475, CVE-2020-8476:
No, exploits of these vulnerabilities cannot affect the integrity of any safety function in System 800xA or Control Builder Safe since no safety certified function depends on the license handling.

CVE-2020-8481, CVE-2020-8479, CVE-2020-8471:
Under certain conditions exploits of this vulnerability may affect the integrity of safety functions in System 800xA. This is however prevented if the Access Enable key in the AC 800M HI is turned Off ("disabled") and Access Level for the variables in the safety applications are configured to "Read Only" or "Confirm and Access Enable" (see *3BNP004865* AC 800M High Integrity Safety Manual* for more information regarding SIL Access Control and Confirmed Write Support).
With other configurations exploits of this vulnerability may affect the integrity of safety functions in System 800xA. This risk could be avoided by changing to the described safe configuration or by following the advice in section "Recommended immediate actions" below.
It can be noted that creating malware that exploits this vulnerability and affects the integrity of a safety function will involve a substantial amount of intricate reverse engineering to circumvent the existing safety measures in AC 800M HI.

Affected product versions in detail

The following table lists the CLS versions and the associated System 800xA versions and indicate which of the vulnerabilities these are affected by.

System 800xA version	CLS version	CVE-2020-8481	CVE-2020-8479	CVE-2020-8475	CVE-2020-8476	CVE-2020-8471
5.1	5.1.0/0 (5.1.0.14)	Y	Y	Y	Y	Y
5.1 Rev A 5.1 Rev B 5.1 Rev B 5.1 Rev C 5.1 FP4 5.1 Rev D/FP4 Rev D	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[1]	Y	Y	Y	Y
5.1 Rev E/FP4 Rev E 5.1 Rev E 5.1 Rev E 5.1 Rev E	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[1]	Y	Y	Y	N

[1] See the Note for CVE-2020-8481 in "Recommended immediate actions" Recommended immediate actions.

6.0 6.0.1 6.0.1 6.0.1 6.0.3 6.0.3 6.0.3 6.0.3	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
6.0.3.3	6.0.3-0 (6.0.03000.192)	N	N	Y	Y	N
6.1	6.1.0-0 (6.1.00000.398)	N	Y	Y	Y	N
6.1	6.1.0-0 (6.1.00100.417)	N	N	Y	Y	N
6.1.1	6.1.1-0 (6.1.01000.502)	N	N	N	N	N

The following table lists the CLS versions and the associated Compact HMI versions and indicate which of the vulnerabilities these are affected by.

Compact HMI version	CLS version	CVE-2020-8481	CVE-2020-8479	CVE-2020-8475	CVE-2020-8476	CVE-2020-8471
5.1 5.1 Rev B 5.1 Rev D/FP4 Rev D	5.1.0/1 (5.1.0.38) 5.1.0-2 (5.1.0.53) 5.1.0-5 (5.1.0.84))	N	Y	Y	Y	Y
6.0.1-1 6.0.3-2	6.0.1-0 (6.0.00100.54) 6.0.3-0 (6.0.03000.73)	N	Y	Y	Y	N

The following table lists the CLS versions and the associated Control Builder Safe versions and indicate which of the vulnerabilities these are affected by.

Control Builder Safe version	CLS version	CVE-2020-8481	CVE-2020-8479	CVE-2020-8475	CVE-2020-8476	CVE-2020-8471
1.0 1.1	5.1.0-5 (5.1.0.84))	N	Y	Y	Y	Y
2.0	6.0.3-0 (6.0.03000.73)	N	Y	Y	Y	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-2020-8481 - ABB CLS - Information Disclosure

CVSS v3.0 Base Score: 9.8 (Critical)
CVSS v3.0 Temporal Score: 8.5 (High)
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R
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:H/E:P/RL:O/RC:R
NVD Summary: https://nvd.nist.gov/vuln/detail/CVE-2020-8481

CVE-2020-8479 - ABB CLS -XXE vulnerability

CVSS v3.0 Base Score:	9.3 (High)
CVSS v3.0 Temporal 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

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
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-2020-8476

CVE-2020-8471 – ABB CLS – Weak File Permissions

CVSS v3.0 Base Score:	7.8 (High)
CVSS v3.0 Temporal Score:	7.5 (High)
CVSS v3.0 Vector:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
CVSS v3.0 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-8471

Recommended immediate actions

All the generic recommendations in the generic Cyber Security Advisory 2PAA121231 apply also for System 800xA, Compact HMI and Control Builder Safe. ABB recommends updating to a corrected version, released for the products in this advisory. Customers unable to install the update are advised to review the Mitigations and Workarounds section for additional advice on how to reduce the risk associated with these vulnerabilities. Additionally, the following actions should be considered:

1. **CVE-2020-8481**:

   The vulnerability in the ABB Central Licensing System was corrected in ABB Central Licensing Server 5.1 Rev A (5.1.0.38).

   Check that the usage of the Access Enable key in AC 800M HI and the configured access level of SIL variables corresponds to the risk analysis. See section “Can functional safety be affected by an exploit of any of these vulnerabilities?” above.

   Please Note: If the affected version, ABB Central Licensing Server 5.1 (5.1.0.14) or earlier is or has been used on the currently used hardware, please contact ABB for further assistance.

2. **CVE-2020-8479**:

   The vulnerability in the ABB Central Licensing System was corrected in the following versions:

   - ABB Central Licensing Server 6.0.3.3 (6.0.03000.192)
   - ABB Central Licensing Server 6.1 RU1 (6.1.00100.417)

   Check that the usage of the Access Enable key in AC 800M HI and the configured access level of SIL variables corresponds to the risk analysis. See section “Can functional safety be affected by an exploit of any of these vulnerabilities?” above.

3. **CVE-2020-8475** and **CVE-2020-8476**:

   The vulnerability in ABB Central Licensing System was corrected in the following version:

   - ABB Central Licensing Server 6.1.1 (6.1.01000.502)

   Check that the usage of the Access Enable key in AC 800M HI and the configured access level of SIL variables correspond to the risk analysis. See section “Can functional safety be affected by an exploit of any of these vulnerabilities?” above.

4. **CVE-2020-8471**:

   The vulnerability in the ABB Central Licensing System was corrected in the following versions;

   - ABB Central Licensing Server 5.1 Rev E (5.1.0.99),
   - ABB Central Licensing Server 6.0 (6.0.0.26)

   Check that the usage of the Access Enable key in AC 800M HI and the configured access level of SIL variables corresponds to the risk analysis. See section “Can functional safety be affected by an exploit of any of these vulnerabilities?” above.

Mitigating factors

For CVE-2020-8479, CVE-2020-8475, 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 System 800xA deployment guidelines and ensure that the system 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 Client Server Network from other networks with firewalls.

For CVE-2020-8481, CVE-2020-8471, a mitigating factor is that an attacker needs to be able to login to an account in the system, so the primary mitigation against these attacks is to ensure that only authorized persons have access to user accounts on the system nodes. This also includes any user accounts accessing the system via remote tools like Remote Desktop. Interactive logon to service accounts should be blocked.

If lot of License annoyance messages are displayed in multiple nodes in the System, this must be investigated in the CLS Server:

a) The ABBLicense website in Internet Information Services (IIS) Manager must be checked if it is online. If it is offline, restart the Application Pool “ABBCLSAppPool” from IIS Manager. The CLS

clients should be able to obtain licenses and the annoyance messages should not be displayed anymore. In case the License server has crashed an investigation is recommended to determine if it was caused by an attack or by some other reason.

b) If the problem is still not resolved, then check the license assignments in the License Assignment Editor. If License assignments are found to be made on invalid or suspicious nodes, then these invalid entries must be deleted. The CLS clients should be able to obtain the blocked licenses and the annoyance messages should not be displayed anymore.

Any suspicious activity from a node in the System network should be investigated.

Workarounds

None.

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	P3 all	Added FAQ question on functional safety Misc clarifications CVE-2020-8479: Updated vulnerability details, recommended immediate actions and CVSS score	2020-04-20
C	P4, P6	Revised with update available for CVE-2020-8475 and CVE-2020-8476	2021-06-14