DOCUMENT ID : 2PAA123981
REVISION : D
DATE: 2022-03-15

CYBERSECURITY ADVISORY

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

CVE IDs: 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 ABB Ability™ Symphony Plus Operations (3.0 to 3.3)

ABB Central Licensing System (CLS) as used in ABB Ability™ Symphony Plus Engineering (1.0 to 2.3).

ABB Central Licensing System (CLS) as used in Composer Harmony (5.1, 6.0, 6.1)

ABB Central Licensing System (CLS) as used in Composer Melody (6.1)

ABB Central Licensing System (CLS) as used in Harmony OPC Server (6.0, 6.1, 7.0)

Important: For more details on which of the vulnerabilities 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 Cybersecurity 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 S+ Operations (3.0 to 3.3), S+ Engineering (1.0 to 2.3), Composer Harmony (5.1, 6.0, 6.1), Composer Melody (6.1), and Harmony OPC Server (6.x, 7.0).

Vulnerability details

ABB is aware that the common Central Licensing System used with Symphony Plus, Composer Harmony, Composer Melody, and Harmony OPC Server contains several vulnerabilities which require user attention:

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. Symphony Plus Operations and Engineering are not affected by this vulnerability
2. **CVE-2020-8479**: XML External Entity Injection vulnerability: An attacker who successfully exploited the vulnerabilities could read arbitrary files from the license server and/or from the network and may also block the license handling. Only Client Server installation of CLS is affected by this vulnerability.
3. **CVE-2020-8475**: Denial of Service vulnerability: An attacker who successfully exploited this vulnerability could block the license handling.
   Only Client-Server installation of CLS is affected by this vulnerability.
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.
   Only Client-Server installation of CLS is affected by this vulnerability.
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.

Recommended immediate actions

All the generic recommendations in the generic Cybersecurity Advisory (2PAA121231) apply also for Symphony Plus, Composer Harmony, Composer Melody and Harmony OPC Server. ABB recommends updating to a corrected version, released for the products in this advisory.

End-users who are unable to install the corrected versions recommended below should immediately look to implement the Mitigation and Workarounds listed below as this will significantly restrict an attacker's ability to compromise these systems.

The following actions are advised:

S+ Operations

S+ Operations version 3.0, 3.1, 3.2 and 3.3 are impacted by 3 of the vulnerabilities contained in this announcement; CVE-2020-8479 - ABB CLS - XXE vulnerability, CVE-2020-8475 – ABB CLS – Denial of Service and CVE-2020-8476 – ABB CLS – Elevation of privilege vulnerability. NOTE - earlier versions of S+ Operations (e.g. 2.1.1, 2.1.2) do not use CLS and are therefore not impacted.

Recommended actions:
ABB advises all customers to review their installations to determine if they are using an impacted system as listed above, no further analysis or tools are needed to make this determination.

Users are advised to upgrade to S+ Operations version 3.3 Service Pack 1.

S+ Engineering

S+ Engineering versions prior to 1.4 (e.g. 1.0, 1.3) are impacted by 4 of the vulnerabilities contained in this announcement; CVE-2020-8479 - ABB CLS - XXE vulnerability, CVE-2020-8475 – ABB CLS – Denial of Service and CVE-2020-8476 – ABB CLS – Elevation of privilege vulnerability, as well as CVE-2020-8471 – ABB CLS – Weak File Permissions.

S+ Engineering versions at, or after 1.4 (e.g. 1.4, 2.0, 2.1, 2.1 SP1, 2.2, 2.3) are impacted by only 3 of the vulnerabilities contained in this announcement; CVE-2020-8479 - ABB CLS - XXE vulnerability, CVE-2020-8475 – ABB CLS – Denial of Service and CVE-2020-8476 – ABB CLS – Elevation of privilege vulnerability.

Recommended actions:
ABB advises all customers to review their installations to determine if they are using an impacted system as listed above, no further analysis or tools are needed to make this determination.

All users of S+ Engineering are advised to upgrade to the latest version:

- SD series and Harmony rack users should upgrade to S+ Engineering version 2.3 Rollup 1
- Melody users should upgrade to S+ Engineering for Melody version 1.4 SP1 RU1 (released August 2021) or S+ Engineering for Melody version 2.0 or later.

Composer Harmony (5.1, 6.0, 6.1)

Composer Harmony is impacted by all 5 of the vulnerabilities contained in this announcement; CVE-2020-8479 - ABB CLS - XXE vulnerability, CVE-2020-8475 – ABB CLS – Denial of Service and CVE-2020-8476 – ABB CLS – Elevation of privilege vulnerability, as well as CVE-2020-8471 – ABB CLS – Weak File Permissions.

Recommended actions:
ABB advises all customers to review their installations to determine if they are using an impacted system as listed above, no further analysis or tools are needed to make this determination.

Users are advised to upgrade to S+ Engineering version 2.3 Rollup 1 as this is not affected.

Composer Melody (6.1)

Composer Melody versions 6.1 is impacted by 4 of the vulnerabilities contained in this announcement; CVE-2020-8479 - ABB CLS - XXE vulnerability, CVE-2020-8475 – ABB CLS – Denial of Service and CVE-2020-8476 – ABB CLS – Elevation of privilege vulnerability, as well as CVE-2020-8471 – ABB CLS – Weak File Permissions

Recommended actions:
ABB advises all customers to review their installations to determine if they are using an impacted system as listed above, no further analysis or tools are needed to make this determination.

Users are advised to upgrade to S+ Engineering for Melody version 2.0 or later.

Harmony OPC Server

Harmony OPC Server versions 6.0, 6.1, and 7.0 are impacted by 1 of the vulnerabilities contained in this announcement; CVE-2020-8471 – ABB CLS – Weak File Permissions.

Recommended actions:
ABB advises all customers to review their installations to determine if they are using an impacted system as listed above, no further analysis or tools are needed to make this determination.

All users with affected versions are advised to upgrade to Harmony OPC Server version 7.0 SP2 or version 7.1 or later.

Vulnerability severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. 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.

S+ Operations

CVE-2020-8479 - ABB CLS - XXE vulnerability

CVSS v3.1 Base Score: 9.4 (Critical)
CVSS v3.1 Temporal Score: 8.6 (High)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L/E:P/RL:W/RC:C
CVSS v3.1 Link: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L/E:P/RL:W/RC:C
NVD Summary: https://nvd.nist.gov/vuln/detail/CVE-2020-8479

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

CVSS v3.1 Base Score: 7.5 (High)
CVSS v3.1 Temporal Score: 6.9 (Medium)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:W/RC:C
CVSS v3.1 Link: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/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 v3.1 Base Score: 7.5 (High)
CVSS v3.1 Temporal Score: 6.9 (Medium)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:W/RC:C
CVSS v3.1 Link: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:W/RC:C

S+ Engineering

CVE-2020-8479 - ABB CLS - XXE vulnerability

CVSS v3.1 Base Score: 9.8 (Critical)
CVSS v3.1 Temporal Score: 9.0 (Critical)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C
CVSS v3.1 Link: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C
NVD Summary: https://nvd.nist.gov/vuln/detail/CVE-2020-8479

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

CVSS v3.1 Base Score: 7.5 (High)
CVSS v3.1 Temporal Score: 6.9 (Medium)

CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:W/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/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 v3.1 Base Score:	7.5 (High)
CVSS v3.1 Temporal Score:	6.9 (Medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:W/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/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 v3.1 Base Score:	7.8 (High)
CVSS v3.1 Temporal Score:	7.5 (High)
CVSS v3.1 Vector:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/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

Composer Harmony

CVE-2020-8481 - ABB CLS - Information Disclosure

CVSS v3.1 Base Score:	9.8 (Critical)
CVSS v3.1 Temporal Score:	8.9 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:R
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:R
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-8481

CVE-2020-8479 - ABB CLS - XXE vulnerability

CVSS v3.1 Base Score:	9.8 (Critical)
CVSS v3.1 Temporal Score:	9.0 (Critical)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-8479

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

CVSS v3.1 Base Score:	7.5 (High)
CVSS v3.1 Temporal Score:	6.9 (Medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:W/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/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 v3.1 Base Score:	7.5 (High)
CVSS v3.1 Temporal Score:	6.9 (Medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:W/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/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 v3.1 Base Score:	7.8 (High)
CVSS v3.1 Temporal Score:	7.5 (High)
CVSS v3.1 Vector:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/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

Composer Melody

CVE-2020-8479 - ABB CLS - XXE vulnerability

CVSS v3.1 Base Score:	9.4 (Critical)
CVSS v3.1 Temporal Score:	8.6 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L/E:P/RL:W/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L/E:P/RL:W/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-8479

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

CVSS v3.1 Base Score:	5.3 (Medium)
CVSS v3.1 Temporal Score:	4.9 (Medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:W/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/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-2020-8479

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

CVSS v3.1 Base Score:	5.3 (Medium)
CVSS v3.1 Temporal Score:	4.9 (Medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:W/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/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-2020-8479

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

CVSS v3.1 Base Score:	7.8 (High)
CVSS v3.1 Temporal Score:	7.5 (High)
CVSS v3.1 Vector:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/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

Harmony OPC Server

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

CVSS v3.1 Base Score: 7.8 (High)
CVSS v3.1 Temporal Score: 7.8 (High)
CVSS v3.1 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:U/RC:C
CVSS v3.1 Link: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:U/RC:C
NVD Summary: https://nvd.nist.gov/vuln/detail/CVE-2020-8471

Affected product versions in detail

The following tables list the CLS versions and the associated product versions that are affected by each vulnerability.

Note: Only Client-Server installations of CLS are affected by CVE-2020-8479, CVE-2020-8475, and CVE-2020-8476. See the generic Cybersecurity Advisory for CLS (2PAA121231) for details.

S+ Operations

S+ Operations version	CLS version	CVE-2020-8479	CVE-2020-8475	CVE-2020-8476	CVE-2020-8471
3.0	6.1.0-0 (6.1.00000.16)	Y	Y	Y	N
3.1 3.1 SP1 3.2 3.3	6.1.0-0 (6.1.00000.18)	Y	Y	Y	N
3.3 SP1	6.1.1-0 (6.1.01000.499)	N	N	N	N

S+ Engineering

S+ Engineering version	CLS version	CVE-2020-8479	CVE-2020-8475	CVE-2020-8476	CVE-2020-8471
1.0 1.0 SP1 1.0 SP2 (Melody) 1.1 1.1 SP1 (Melody) 1.1 SP2 (Melody) 1.1 SP3 (Melody)	5.1.0-4 (5.1.0.70)	Y	Y	Y	Y
1.2 1.3	5.1.0-4 (5.1.0.70)	Y	Y	Y	Y
1.4 1.4 (Melody)	6.1.0-0 (6.1.00000.18)	Y	Y	Y	N
1.4 SP1 RU1 (Melody)	6.1.1-0 (6.1.01000.502)	N	N	N	N
2.0 (Melody)	6.1.1-0 (6.1.01000.492)	N	N	N	N
2.0	6.1.0-0 (6.1.00000.16)	Y	Y	Y	N

S+ Engineering version	CLS version	CVE-2020-8479	CVE-2020-8475	CVE-2020-8476	CVE-2020-8471
2.1 2.1 SP1 2.3	6.1.0-0 (6.1.00000.18)	Y	Y	Y	N
2.3 RU1	6.1.1-0 (6.1.01000.499)	N	N	N	N

Composer Harmony

Composer Harmony version	CLS version	CVE-2020-8481	CVE-2020-8479	CVE-2020-8475	CVE-2020-8476	CVE-2020-8471
5.1	5.1.0/1 (5.1.0.35)	Y	Y	Y	Y	Y
6.0	5.1.0/1 (5.1.0.38)	N	Y	Y	Y	Y
6.1	5.1.0-4 (5.1.0.70)	N	Y	Y	Y	Y

Composer Melody

Composer Melody version	CLS version	CVE-2020-8479	CVE-2020-8475	CVE-2020-8476	CVE-2020-8471
6.1	5.1.0-4 (5.1.0.70)	Y	Y	Y	Y

Harmony OPC Server

Harmony OPC Server version	CLS version	CVE-2020-8471
6.0 6.0 SP1 6.1 7.0 7.0 SP1	5.1.0-4 (5.1.0.70)	Y
7.0 SP2	6.1.1-0 (6.1000.496)	N
7.1	6.1.1-0 (6.1.01000.499)	N

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 respective products 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 (if supported) and by separating the Client-Server Network from other networks with firewalls.

For CVE-2020-8481 and 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.

Workarounds

No workaround is available for S+ Operations and S+ Engineering when used in a **multi-node system** context. If either of the products is used in a **single-node only** context, the exposure to issues CVE-2020-8479, CVE-2020-8475, and CVE-2020-8476 can be prevented by installing CLS in Standalone mode instead of Client-Server (see the Summary section in the generic Cybersecurity Advisory for CLS, 2PAA121231).

The exposure of Composer Harmony and Composer Melody to issues CVE-2020-8479, CVE-2020-8475, and CVE-2020-8476 can be prevented by installing CLS in Standalone mode instead of Client-Server (see the Summary section in the generic Cybersecurity Advisory for CLS, 2PAA121231).

No workaround is available for Harmony OPC Server.

Frequently asked questions

How is Symphony Plus as a system affected by the vulnerabilities?

The exploitation of the CLS vulnerabilities may block normal license handling and more, as described above. However, in a Symphony Plus system the effect of these can differ in a significant way.

Note: The CLS Standalone (SA) installation contains less vulnerabilities than the Client-Server installation (see 2PAA121231 for details). Although the CLS SA is supported, the following notes describe how Symphony Plus can be affected for all the reported CLS vulnerabilities and possible described threats.

A Symphony Plus system consists of three main functional areas:

1. S+ Operations

   a) Deals with typical 24/7 operational tasks. The S+ Operations server checks for the license at the startup only. If the license handling is blocked due to the exploit of a CLS vulnerability, the S+ Operations behavior is different depending on the following scenarios:
   b) S+ Operations is already running when the CLS gets compromised: This does not affect the server operational continuity. The server availability is not compromised.
   c) CLS is not available when S+ Operations is started: In this case it will be closed later. The server availability is compromised.
   d) CLS is available but license handling is blocked: When S+ Operations is started, it will connect to the CLS and won't get closed but all drivers for data acquisition (and other licensed features) will not work. The server availability is compromised.

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

1. 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.
2. 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.

3. S+ Operations History (as included in S+ Operations)
   a) Deals with typical 24/7 operational and data recording tasks. The S+ Operations History server checks for the license at the startup, on a periodical basis (maintenance purpose) and every time a licensed feature is used. If the license handling is blocked due to the exploit of a CLS vulnerability, the S+ Operations History server licensed functionalities are affected and may not work.
   b) This means, the S+ Operations History server availability is compromised but this will not affect the S+ Operations main server availability.
4. S+ Engineering
   a) Deals with typical engineering and configuration tasks. The S+ Engineering Workbench tool checks for the license both at the startup and every time a licensed feature is required. If the license handling is blocked due to the exploit of a CLS vulnerability, the tool does not start, or no licensed features can be used.
   b) This loss of availability affects the engineering and configuration of the system only.
   c) **Note:** The vulnerabilities described in this document do not apply to the standalone ABB product S+ Historian.

How is Composer Harmony affected by the vulnerabilities?

Composer Harmony deals with typical engineering and configuration tasks. It checks for the license both at the startup and periodically thereafter. If the license handling is blocked due to the exploit of a CLS vulnerability, the Composer Harmony will not open a project and none of its functionality is available.

How is Composer Melody affected by the vulnerabilities?

Composer Melody deals with typical engineering and configuration tasks. It checks for the license both at the startup and periodically thereafter. If the license handling is blocked due to the exploit of a CLS vulnerability, there is no loss of availability and the Composer Melody functionality is available. There are two exceptions:

1. Enabling slow Fnet communication on new Melody controllers (like PM877)
2. Enabling Modbus TCP on PM877 Melody controller

These two features are bound to a license with counter and are checked each time the user tries to apply these configurations. This means that in case the license handling is blocked, users cannot configure additional controllers with slow Fnet or Modbus TCP (both configurations are typically changed during a commissioning phase, not in a running plant).

How is Harmony OPC Server affected by the vulnerabilities?

The Harmony OPC Server checks for the license both at the startup and periodically thereafter. If the license handling is blocked due to the exploit of a CLS vulnerability, there is no loss of availability and the Harmony OPC Server functionality is available (Harmony OPC server just logs error messages).

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	2020-12-14
B	various	Updated to resolve planned dates to actual Composer Melody 5.3 is not affected and removed	2021-06-30
C	Page 3 & 4	S+ Engineering for Melody version 1.4 SP1 RU1 had planned date is now released August 2021. Also S+ Engineering 2.0 or later is released and recommend.	2022-03-04
D	Page 4 & 9	Updated Harmony OPC Server details to clarify that version 7.1 (like 7.0 SP2) is also NOT affected so it is a recommend update to resolve the vulnerability. Also added the CLS license version of version 7.1 and corrected 7.0.	2022-03-15