DOCUMENT ID: 4HZM000603
REVISION: B
DATE: 2025-11-28

CYBER SECURITY ADVISORY

ABB Ability Camera Connect Vulnerabilities in outdated 3rd party component (VLC)

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.

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 Ability Camera Connect 1.5.0.14 and below

Vulnerability IDs

CVE-2024-46461; CVE-2023-47360; CVE-2023-47359; CVE-2023-46814; CVE-2022-41325; CVE-2020-26664; CVE-2019-19721; CVE-2019-13962; CVE-2019-13615; CVE-2019-13602; CVE-2019-5460; CVE-2019-5459; CVE-2019-5439; CVE-2018-11529; CVE-2017-17670; CVE-2017-10699; CVE-2017-9301; CVE-2017-9300; CVE-2017-8313; CVE-2017-8312; CVE-2017-8311; CVE-2017-8310

Summary

ABB is aware of public reports of vulnerabilities in a 3rd party component VLC media player Version 2.2.4 which was delivered together with the installation package of Camera Connect Version 1.5.0.14 and below. An update is available that resolves a privately reported outdated 3rd party component with vulnerabilities in the product versions listed above.

An attacker who successfully exploited any of these vulnerabilities in the 3rd party component could potentially compromise the system in different ways.

Recommended immediate actions

The problem is corrected in the following product versions:

ABB Ability Camera Connect 1.5.0.15

The 3rd party component has already been updated. The easiest path to mitigate the problem is an update of just VLC Media Player by the customer. ABB recommends that customers apply the update at earliest convenience.

It is also possible to update to the latest Version of Camera Connect.

Vulnerability severity and details

Vulnerabilities existent in the 3rd party component VLC Media player included in the product versions listed above.

The following CVEs and their descriptions where consulted in the CVE[1] website as well as the Common Vulnerability Scoring System (CVSS) for both v3.1[2] and v4.0[3] and the indicated Common Weakness Enumerations (CWE).

CVE-2024-46461[4]

VLC media player 3.0.20 and earlier is vulnerable to denial of service through an integer overflow which could be triggered with a maliciously crafted mms stream (heap based overflow). If successful, a malicious third party could trigger either a crash of VLC or an arbitrary code execution with the target user's privileges.

CVSS

CVSS v3.1 Base Score:	8.0
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-122	Heap-based Buffer Overflow

Mitigating Factor

The VLC-based component operates solely within completely isolated environments without internet access or any connectivity to external networks. Consequently:

- **No exposure to untrusted MMS streams**: The integer overflow vulnerability relies on handling a maliciously crafted external stream, which is not possible in isolated environments.

[1] www.cve.org

[2] For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. 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.

[3] For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations' computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

[4] https://www.cve.org/CVERecord?id=CVE-2024-46461

- **No remote attacker access**: Without network ingress, attackers cannot trigger the vulnerability remotely.
- **Drastically reduced attack surface**: The absence of any external media inputs effectively neutralizes the exploit path, significantly lowering the risk of both denial of service and code execution.

CVE-2023-47360[5]

Videolan VLC prior to version 3.0.20 contains an Integer underflow that leads to an incorrect packet length.

CVSS

CVSS v3.1 Base Score:	7.5
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-191	Integer Underflow (Wrap or Wraparound)

Mitigating Factor

- **Air-gapped environments only:** Camera Connect is deployed in completely isolated environments lacking any network connectivity or internet access.
- **No exposure to MMS streams:** The vulnerability depends on processing crafted MMS streams, which cannot originate from external or internal network sources when the system is air-gapped.
- **Elimination of remote attack surface:** Without any method for an attacker to deliver malicious media inputs, the vulnerability cannot be triggered remotely.
- **Strong reduction in exploitation risk:** The combined absence of external media ingestion and unavailable network paths effectively neutralizes the integer underflow exploit, significantly reducing the likelihood of both denial-of-service and memory corruption scenarios.

CVE-2023-47359[6]

Videolan VLC prior to version 3.0.20 contains an incorrect offset read that leads to a Heap-Based Buffer Overflow in function GetPacket() and results in a memory corruption.

CVSS

CVSS v3.1 Base Score:	9.8
CVSS v3.1 Temporal Score:	N/A

[5] https://www.cve.org/CVERecord?id=CVE-2023-47360

[6] https://www.cve.org/CVERecord?id=CVE-2023-47359

CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-787	Out-of-bounds Write

Mitigating Factor
Given that Camera Connect is deployed exclusively in fully isolated, air-gapped environments with no internet access or external network connectivity, the following risk-reduction factors apply:

- **No exposure to crafted MMS streams:** The exploit requires the receipt of specially crafted packets via the MMS protocol, which cannot occur without network connectivity.
- **Network attack vector eliminated:** As the vulnerability's CVSS vector highlights a network-based attack (AV:N), the lack of any ingress network path nullifies the attack surface.
- **Low likelihood of exploitation:** Without access to malicious media input, there is effectively no practical method for an attacker to trigger memory corruption, making the likelihood of denial of service or arbitrary code execution negligible.

CVE-2023-46814[7]

A binary hijacking vulnerability exists within the VideoLAN VLC media player before 3.0.19 on Windows. The uninstaller attempts to execute code with elevated privileges out of a standard user writable location. Standard users may use this to gain arbitrary code execution as SYSTEM.

CVSS

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-427	Uncontrolled Search Path Element

Mitigating Factor
Given that the VLC-based component is installed **exclusively** within **air-gapped environments** under **strict administrative control**, the following factors substantially reduce risk:

- **Restricted user access**: Only trusted, privileged users perform installations and modifications. Standard users have no write permissions to the uninstaller directory.
- **No internet or network access**: The exploit requires local manipulation of VLC's uninstaller files; without external connectivity, remote coercion or manipulation is impossible.

[7] https://www.cve.org/CVERecord?id=CVE-2023-46814

- **Elimination of attacker vector**: In air-gapped deployments with administrative controls, unprivileged users cannot place malicious DLLs or executables in the uninstaller's search path.
- **Minimized privilege escalation risk**: The combination of controlled write access, absence of network exposure, and trusted user roles effectively neutralizes the binary hijacking threat, rendering successful exploitation highly unlikely.

CVE-2022-41325[8]

An integer overflow in the VNC module in VideoLAN VLC Media Player through 3.0.17.4 allows attackers, by tricking a user into opening a crafted playlist or connecting to a rogue VNC server, to crash VLC or execute code under some conditions.

CVSS

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-190	Integer Overflow or Wraparound

Mitigating Factor
Camera Connect is deployed exclusively in **air-gapped environments** with **no internet connectivity or external network access**, which significantly reduces the risk:

- **No exposure to malicious MKV files:** The exploit requires a specially crafted Matroska file. In controlled environments without external media sources, such files cannot be introduced.
- **Remote attack vector eliminated:** The vulnerability's CVSS vector indicates a network-based attack scenario, which is impossible without connectivity.
- **Strict operational controls:** Media ingestion is limited to trusted sources under administrative supervision, further minimizing the likelihood of malicious file introduction.
- **Effective risk reduction:** These combined factors render exploitation highly improbable, neutralizing the buffer overflow threat.

CVE-2020-26664[9]

A vulnerability in EbmlTypeDispatcher::send in VideoLAN VLC media player 3.0.11 allows attackers to trigger a heap-based buffer overflow via a crafted .mkv file.

CVSS

CVSS v3.1 Base Score:	7.8

[8] https://www.cve.org/CVERecord?id=CVE-2022-41325

[9] https://www.cve.org/CVERecord?id=CVE-2020-26664

CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-787	Out-of-bounds Write

Mitigating Factor

- **No exposure to malicious ASF files:** The exploit requires a specially crafted ASF file. In controlled environments without external media sources, such files cannot be introduced.
- **Remote attack vector eliminated:** The vulnerability's CVSS vector indicates a network-based attack scenario, which is impossible without connectivity.
- **Strict operational controls:** Media ingestion is limited to trusted sources under administrative supervision, further minimizing the likelihood of malicious file introduction.
- **Effective risk reduction:** These combined factors render exploitation highly improbable, neutralizing the buffer overflow threat.

CVE-2019-19721[10]

An off-by-one error in the DecodeBlock function in codec/sdl_image.c in VideoLAN VLC media player before 3.0.9 allows remote attackers to cause a denial of service (memory corruption) via a crafted image file. NOTE: this may be related to the SDL_Image product.

CVSS

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-193	Off-by-one Error
CWE-787	Out-of-bounds Write

Mitigating Factor

- **No exposure to malicious ASF files:** The exploit requires a specially crafted ASF file. In controlled environments without external media sources, such files cannot be introduced.
- **Remote attack vector eliminated:** The vulnerability's CVSS vector indicates a network-based attack scenario, which is impossible without connectivity.
- **Strict operational controls:** Media ingestion is limited to trusted sources under administrative supervision, further minimizing the likelihood of malicious file introduction.

[10] https://www.cve.org/CVERecord?id=CVE-2019-19721

- **Effective risk reduction:** These combined factors render exploitation highly improbable, neutralizing the buffer overflow threat.

CVE-2019-13962[11]

lavc_CopyPicture in modules/codec/avcodec/video.c in VideoLAN VLC media player through 3.0.7 has a heap-based buffer over-read because it does not properly validate the width and height.

CVSS

CVSS v3.1 Base Score:	9.8
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-125	Out-of-bounds Read

Mitigating Factor

- **No exposure to malicious MKV files:** The exploit requires a specially crafted MKV file. In controlled environments without external media sources, such files cannot be introduced.
- **Remote attack vector eliminated:** The vulnerability's CVSS vector indicates a network-based attack scenario, which is impossible without connectivity.
- **Strict operational controls:** Media ingestion is limited to trusted sources under administrative supervision, further minimizing the likelihood of malicious file introduction.
- **Effective risk reduction:** These combined factors render exploitation highly improbable, neutralizing the buffer overflow threat.

CVE-2019-13615[12]

libebml before 1.3.6, as used in the MKV module in VideoLAN VLC Media Player binaries before 3.0.3, has a heap-based buffer over-read in EbmlElement::FindNextElement.

CVSS

CVSS v3.1 Base Score:	5.5
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

[11] https://www.cve.org/CVERecord?id=CVE-2019-13962

[12] https://www.cve.org/CVERecord?id=CVE-2019-13615

CWE

CWE-125	Out-of-bounds Read

Mitigating Factor

- **No exposure to malicious ASF files:** The exploit requires a specially crafted ASF file. In controlled environments without external media sources, such files cannot be introduced.
- **Remote attack vector eliminated:** The vulnerability's CVSS vector indicates a network-based attack scenario, which is impossible without connectivity.
- **Strict operational controls:** Media ingestion is limited to trusted sources under administrative supervision, further minimizing the likelihood of malicious file introduction.
- **Effective risk reduction:** These combined factors render exploitation highly improbable, neutralizing the buffer overflow threat.

CVE-2019-13602[13]

An Integer Underflow in MP4_EIA608_Convert() in modules/demux/mp4/mp4.c in VideoLAN VLC media player through 3.0.7.1 allows remote attackers to cause a denial of service (heap-based buffer overflow and crash) or possibly have unspecified other impact via a crafted .mp4 file.

CVSS

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-787	Out-of-bounds Write

Mitigating Factor

- **No exposure to malicious ASF files:** The exploit requires a specially crafted ASF file. In controlled environments without external media sources, such files cannot be introduced.
- **Remote attack vector eliminated:** The vulnerability's CVSS vector indicates a network-based attack scenario, which is impossible without connectivity.
- **Strict operational controls:** Media ingestion is limited to trusted sources under administrative supervision, further minimizing the likelihood of malicious file introduction.
- **Effective risk reduction:** These combined factors render exploitation highly improbable, neutralizing the buffer overflow threat.

[13] https://www.cve.org/CVERecord?id=CVE-2019-13602

CVE-2019-5460[14]

Double Free in VLC versions <= 3.0.6 leads to a crash.

CVSS

CVSS v3.1 Base Score:	5.5
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-415	Double Free

Mitigating Factor

- **No exposure to malicious ASF files:** The exploit requires a specially crafted ASF file. In controlled environments without external media sources, such files cannot be introduced.
- **Remote attack vector eliminated:** The vulnerability's CVSS vector indicates a network-based attack scenario, which is impossible without connectivity.
- **Strict operational controls:** Media ingestion is limited to trusted sources under administrative supervision, further minimizing the likelihood of malicious file introduction.
- **Effective risk reduction:** These combined factors render exploitation highly improbable, neutralizing the buffer overflow threat.

CVE-2019-5459[15]

An Integer underflow in VLC Media Player versions < 3.0.7 leads to an out-of-band read.

CVSS

CVSS v3.1 Base Score:	7.3
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-191	Integer Underflow (Wrap or Wraparound)

[14] https://www.cve.org/CVERecord?id=CVE-2019-5460

[15] https://www.cve.org/CVERecord?id=CVE-2019-5459

Mitigating Factor

- **No exposure to malicious ASF files:** The exploit requires a specially crafted ASF file. In controlled environments without external media sources, such files cannot be introduced.
- **Remote attack vector eliminated:** The vulnerability's CVSS vector indicates a network-based attack scenario, which is impossible without connectivity.
- **Strict operational controls:** Media ingestion is limited to trusted sources under administrative supervision, further minimizing the likelihood of malicious file introduction.
- **Effective risk reduction:** These combined factors render exploitation highly improbable, neutralizing the buffer overflow threat.

CVE-2019-5439[16]

A Buffer Overflow in VLC Media Player < 3.0.7 causes a crash which can possibly be further developed into a remote code execution exploit.

CVSS

CVSS v3.1 Base Score:	6.5
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Mitigating Factor

- **No exposure to malicious ASF files:** The exploit requires a specially crafted ASF file. In controlled environments without external media sources, such files cannot be introduced.
- **Remote attack vector eliminated:** The vulnerability's CVSS vector indicates a network-based attack scenario, which is impossible without connectivity.
- **Strict operational controls:** Media ingestion is limited to trusted sources under administrative supervision, further minimizing the likelihood of malicious file introduction.
- **Effective risk reduction:** These combined factors render exploitation highly improbable, neutralizing the buffer overflow threat.

CVE-2018-11529[17]

VideoLAN VLC media player 2.2.x is prone to a use after free vulnerability which an attacker can leverage to execute arbitrary code via crafted MKV files. Failed exploit attempts will likely result in denial of service conditions.

[16] https://www.cve.org/CVERecord?id=CVE-2019-5439

[17] https://www.cve.org/CVERecord?id=CVE-2018-11529

CVSS

CVSS v3.1 Base Score:	8.0
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-416	Use After Free

Mitigating Factor

The affected software is deployed exclusively in isolated environments with no internet connectivity and restricted external access. Exploitation of this vulnerability requires a user to open a specially crafted MKV file provided by an attacker. Since the system operates in a controlled network without exposure to untrusted sources, the likelihood of receiving and executing malicious media files is significantly reduced. Additionally, operational procedures can enforce the use of trusted media files only, further minimizing the risk.

CVE-2017-17670[18]

In VideoLAN VLC media player through 2.2.8, there is a type conversion vulnerability in modules/demux/mp4/libmp4.c in the MP4 demux module leading to a invalid free, because the type of a box may be changed between a read operation and a free operation.

CVSS

CVSS v3.1 Base Score:	8.8
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-416	Use After Free

Mitigating Factor

The affected VLC component is deployed exclusively in fully isolated, air-gapped environments with no internet connectivity and tightly controlled external sources. Exploitation of CVE-2017-17670 requires a user to open a specifically crafted MP4 file containing a type-conversion error in the demuxer. Since the system only processes trusted media files—validated through internal procedures and secured media

[18] https://www.cve.org/CVERecord?id=CVE-2017-17670

channels—the probability of exposure to hostile MP4 content is minimal. Therefore, the risk of successful exploitation is significantly mitigated by the restricted deployment context.

CVE-2017-10699[19]

avcodec 2.2.x, as used in VideoLAN VLC media player 2.2.7-x before 2017-06-29, allows out-of-bounds heap memory write due to calling memcpy() with a wrong size, leading to a denial of service (application crash) or possibly code execution.

CVSS

CVSS v3.1 Base Score:	9.8
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-787	Out-of-bounds Write

Mitigating Factor
No network-based exposure: The vulnerability requires an external actor to supply malicious media content. With no Internet connectivity and presumably controlled file sources, the risk of loading untrusted files is minimal.

CVE-2017-9301[20]

plugins\audio_filter\libmpgatofixed32_plugin.dll in VideoLAN VLC media player 2.2.4 allows remote attackers to cause a denial of service (invalid read and application crash) or possibly have unspecified other impact via a crafted file.

CVSS

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

[19] https://www.cve.org/CVERecord?id=CVE-2017-10699

[20] https://www.cve.org/CVERecord?id=CVE-2017-9301

CWE-125	Out-of-bounds Read

Mitigating Factor
This vulnerability affects the libmpgatofixed32_plugin.dll module in VLC 2.2.4, which is responsible for decoding MPEG audio streams. The software in question does **not process audio files or use any functionality related to audio decoding**, meaning the vulnerable component is never invoked during normal operation. Additionally, the deployment environment is **fully offline with no internet connectivity**, and media ingestion is restricted to trusted internal sources.
As a result, the attack surface for this vulnerability is effectively **nonexistent**, and the risk of exploitation is **negligible** under these conditions.

CVE-2017-9300[21]

plugins\codec\libflac_plugin.dll in VideoLAN VLC media player 2.2.4 allows remote attackers to cause a denial of service (heap corruption and application crash) or possibly have unspecified other impact via a crafted FLAC file.

CVSS

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer

Mitigating Factor
This vulnerability affects VLC's FLAC audio processing component. Camera Connect does **not handle or process audio files**, meaning the vulnerable code path is never executed during normal operation. Combined with the fact that the deployment environment is fully isolated (air-gapped) and does not allow external file transfers from untrusted sources, the likelihood of exploitation is effectively eliminated.

CVE-2017-8313[22]

Heap out-of-bound read in ParseJSS in VideoLAN VLC before 2.2.5 due to missing check of string termination allows attackers to read data beyond allocated memory and potentially crash the process via a crafted subtitles file.

CVSS

CVSS v3.1 Base Score:	5.5

[21] https://www.cve.org/CVERecord?id=CVE-2017-9300

[22] https://www.cve.org/CVERecord?id=CVE-2017-8313

CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-125	Out-of-bounds Read

Mitigating Factor
Even though the affected VLC version (2.2.4) contains this vulnerability, the software is deployed in fully air-gapped environments with no external or internet-facing connectivity. As a result, the likelihood of exploiting this vulnerability is extremely low.

CVE-2017-8312[23]

Heap out-of-bound read in ParseJSS in VideoLAN VLC due to missing check of string length allows attackers to read heap uninitialized data via a crafted subtitles file.

CVSS

CVSS v3.1 Base Score:	5.5
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-125	Out-of-bounds Read

Mitigating Factor
Because the affected VLC version (2.2.4) suffers from a heap out-of-bound read in the ParseJSS function—allowing an attacker to read uninitialized heap data via a crafted subtitles file—the risk of external exploitation is significantly reduced in your environment. Since the software is installed in strictly isolated systems with **no internet access**, no external attacker can deliver malicious subtitle files remotely. Consequently, the only remaining exposure is local: an insider would need to intentionally load a crafted subtitle file to trigger the issue—a scenario considered highly unlikely under current governance and usage controls.

[23] https://www.cve.org/CVERecord?id=CVE-2017-8312

CVE-2017-8311[24]

Potential heap based buffer overflow in ParseJSS in VideoLAN VLC before 2.2.5 due to skipping NULL terminator in an input string allows attackers to execute arbitrary code via a crafted subtitles file.

CVSS

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer

Mitigating Factor
Since the application is deployed exclusively in isolated, air-gapped environments with no external network connectivity, the **attack vector**—specifically, the ability for an attacker to deliver a crafted subtitle file—is significantly constrained.

CVE-2017-8310[25]

Heap out-of-bound read in CreateHtmlSubtitle in VideoLAN VLC 2.2.x due to missing check of string termination allows attackers to read data beyond allocated memory and potentially crash the process (causing a denial of service) via a crafted subtitles file.

CVSS

CVSS v3.1 Base Score:	5.5
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-125	Out-of-bounds Read

Mitigating Factor
Because your team's VLC-based software is deployed **only in isolated environments without internet access**, the risk of malicious delivery of crafted subtitle files is greatly diminished. This significantly reduces exploitation likelihood.

[24] https://www.cve.org/CVERecord?id=CVE-2017-8311

[25] https://www.cve.org/CVERecord?id=CVE-2017-8310

Frequently asked questions

What causes the vulnerability?

The vulnerability is caused by unchecked input data in the VLC media player in Camera Connect

What is <affected product or component>?

VLC media player

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the affected system node to stop or become inaccessible and allow the attacker to insert and run arbitrary code .

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted file, copying the file to affected system nodes and then manually open the file via VLC Mediaplayer. 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. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

No, to exploit this vulnerability an attacker would need to have physical access to an affected system node.

Can functional safety be affected by an exploit of this vulnerability?

While these vulnerabilities primarily impact confidentiality, integrity, and availability, they do not directly affect functional safety in the traditional sense. However, a compromised system (due to arbitrary code execution or a critical service crash) may compromise safety-related processes dependent on VLC, potentially disrupting business operations or compliance.

What does the update do?

The update removes the vulnerability by providing a newer version of the VLC media player

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

This vulnerability has been publicly disclosed for the 3rd party component, but not for the ABB product using this component

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 issued.

General security recommendations

For any installation of software-related ABB products we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g. office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date in terms of installed software, operating system, and firmware patches as well as anti-virus and firewall.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

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 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	27/Nov/2025
B	References	Removing references	28/Nov/2025