1 Advisory Information

- **Advisory ID:** BOSCH-SA-464066-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2022-32540
    - Base Score: 7.4 (High)
- **Published:** 21 Sep 2022
- **Last Updated:** 21 Sep 2022

2 Summary

BVMS Operator Client application or the VIDEOJET Decoder VJD-7513 may receive an *unencrypted* live-stream from a camera which allows a man-in-the-middle attacker to compromise the confidential video streams.

This happens only in combination with cameras of platform CPP13 or CPP14.x when encrypted UDP connection is configured. Please be aware that encrypted UDP connection is default setting («Secure Connection» setting) for all cameras added into BVMS.

Decoders used in BVMS system are only affected when BVMS version is higher or equal to 10.1.0 as older BVMS versions do not support UDP connection between camera and decoder. Standalone decoders are only affected, when the Secure flag and UDP multicast is selected for camera streams.

For more details please see the description of the vulnerability in this advisory.

Bosch rates this vulnerability with CVSSv3.1 base score 7.4 (High), where the final rating depends on the customer's environment.

Customers are strongly advised to update the software to the fixed versions or consider listed mitigations.

3 Affected Products

- Bosch BVMS 10.1 <= 10.1.1
- Bosch BVMS 11.0 <= 11.0.0
- Bosch BVMS 11.1 <= 11.1.0
- Bosch VJD-7513 10.23.0002
- Bosch VJD-7513 10.30.0005

4 Solution and Mitigations

4.1 Software Updates

The recommended approach is to update the affected Bosch software and hardware firmware to fixed versions. Please refer to appendix for list of affected versions and available updates.

A reboot is required after applying the update to BVMS. To check whether the update has been successfully applied, please check the version in Configuration Client or Operator Client menu «Help» -> «About...» -> «Version».

If the update is not applicable in a target environment, users are recommended to follow the mitigations described in the following section.

4.2 Update Operator Client Only

In case the whole BVMS system cannot be updated to the latest version, it is sufficient to update the Operator Client workstations to version 11.1.1 that is fixing this issue and ensuring backwards compatibility. The Update of the Operator Client has to be done on each machine manually as there is no automatic deployment from central BVMS Central Server.

4.3 Use TCP Encryption instead of UDP

When software update is not possible, customers are advised to configure their BVMS systems to use TCP protocol:

- For cameras using workstation settings in Configuration Client. This will force TCP protocol for all cameras, even if they are not affected by the vulnerability described in this advisory.
- For cameras using camera specific context menu in Operator Client to enable TCP protocol for affected cameras only. This is one-time action that has to be made per camera for each BVMS user.
- For decoders using Decoder settings dialog in Configuration Client to use TCP video stream.

To learn more about configuring TCP settings in BVMS Configuration Client see BVMS Configuration Manual:

- Chapter «Workstation Page» -> «Settings Page» (12.7.5)
- Chapter «Edit Encoder/ Edit Decoder Page» (12.8.2)

To learn more about configuring TCP settings in BVMS Operator Client see BVMS Operation Manual:

- Chapter «Using TCP for reliable connection» (6.33)

In case TCP encryption is not feasible in customers environment due to the number of cameras, customers are advised to contact Customer Support.

4.4 Secure Network from Unauthorized Access

It is advised to secure network infrastructure devices including routers, firewalls, switches and prevent unauthorized actors from being able to monitor, modify and deny traffic to and from devices and services inside the customer network. Network administrators should implement following recommendations in conjunction with laws, regulations and industry best practices:

- Segment and segregate networks.
- Harden network management devices by testing patches, turning off unnecessary services on routers and switches, and enforcing strong password policies.
- Monitor the network and review logs.
- Validate integrity of hardware.

5 Vulnerability Details

5.1 CVE-2022-32540

CVE description: Information Disclosure in Operator Client application in BVMS 10.1.1, 11.0 and 11.1.0 and VIDEOJET Decoder VJD-7513 versions 10.23 and 10.30 allows man-in-the-middle attacker to compromise confidential video stream.

This is only applicable for UDP encryption when target system contains cameras with platform CPP13 or CPP14 and firmware version 8.x.

- Problem Type:
  - CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
- CVSS Vector String: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
  - Base Score: 7.4 (High)

6 Remarks

6.1 Security Update Information

With respect to Directive (EU) 2019/770 and Directive (EU) 2019/771 and their national transposition laws, please note:

It is your responsibility to download and/or install any security updates provided by us, for example to maintain product or data security. If you fail to install a security update provided to you within a reasonable period of time, we will not be liable for any product defect solely due to the absence of such security update.

Alternatively, we are entitled to directly download and/or install security updates regardless of your settings. In these cases, we will provide you with the relevant information, e.g. in this security advisory.

6.2 CVSS Scoring

Vulnerability classification has been performed using the CVSS v3.1 scoring system. The CVSS environmental score is specific to each customer's environment and should be defined by the customer to attain a final scoring.

7 Additional Resources

- [1] BVMS Download Area: https://downloadstore.boschsecurity.com/index.php?type=BVMS
- [2] BVMS Viewer Download Area: https://downloadstore.boschsecurity.com/index.php?type=BVMSVWR
- [3] BVMS Appliances (DIVAR IP) Download Area: https://downloadstore.boschsecurity.com/?type=DIPBVMS
- [4] VJD Download Area: https://downloadstore.boschsecurity.com/?type=DEC

Please contact the Bosch PSIRT if you have feedback, comments, or additional information about this vulnerability at: psirt@bosch.com.

8 Revision History

- 21 Sep 2022: Initial Publication

9 Appendix

9.1 Affected Products

9.1.1 BVMS

Affected versions	Name of version to fix the vulnerability
11.1.0	BVMS 11.1.1 Lite-Plus-Professional Setup
11.0.0.1025	BVMS 11.1.1 Lite-Plus-Professional Setup
10.1.1.12	BVMS 11.1.1 Lite-Plus-Professional Setup
10.0 and below	Cameras with CPP13/14 platforms are not supported. When such cameras are added into BVMS system, consider to follow update/mitigation instructions.

BVMS Download Area

9.1.2 BVMS Viewer

Affected versions	Name of version to fix the vulnerability
11.1.0	BVMS Viewer 11.1.1 Setup
11.0.0.1025	BVMS Viewer 11.1.1 Setup
10.1.1.12	BVMS Viewer 11.1.1 Setup

BVMS Viewer Download Area

9.1.3 Bosch DIVAR IP all-in-one 7000 R3

Affected BVMS versions	Name of version to fix the vulnerability
11.0.0.1025	DIP-73_Installer_for_BVMS11.1.1.zip
10.1.1.12	DIP-73_Installer_for_BVMS11.1.1.zip

BVMS Appliances Download Area

9.1.4 Bosch DIVAR IP 7000 R2

Affected BVMS versions	Name of version to fix the vulnerability
11.0.0.1025	BVMS 11.1.1 Lite-Plus-Professional Setup
10.1.1.12	BVMS 11.1.1 Lite-Plus-Professional Setup

BVMS Download Area

9.1.5 Bosch DIVAR IP all-in-one 5000

Affected BVMS versions	Name of version to fix the vulnerability
11.0.0.1025	BVMS 11.1.1 Lite-Plus-Professional Setup
10.1.1.12	BVMS 11.1.1 Lite-Plus-Professional Setup

BVMS Download Area

9.1.6 Bosch DIVAR IP all-in-one 7000

Affected BVMS versions	Name of version to fix the vulnerability
11.0.0.1025	BVMS 11.1.1 Lite-Plus-Professional Setup
10.1.1.12	BVMS 11.1.1 Lite-Plus-Professional Setup

BVMS Download Area

9.1.7 Bosch VIDEOJET Decoder VJD-7513

Affected VJD-7513 firmware	Name of version to fix the vulnerability
10.30.0005	10.31.0005
10.23.0002	10.31.0005

VIDEOJET Decoder Download Area

9.2 Material Lists

9.2.1 BVMS

Family Name	CTN	SAP#	Material description
BVMS Professional 11.1	MBV-BPRO	F.01U.393.647	License Professional base
BVMS Plus 11.1	MBV-BPLU	F.01U.393.650	License Plus base
BVMS Viewer 11.1	MBV-BVWR	F.01U.393.649	License Viewer base
BVMS Lite 11.1	MBV-BLIT	F.01U.393.648	License Lite base
BVMS Professional 11.0	MBV-BPRO	F.01U.393.647	License Professional base
BVMS Plus 11.0	MBV-BPLU	F.01U.393.650	License Plus base
BVMS Viewer 11.0	MBV-BVWR	F.01U.393.649	License Viewer base
BVMS Lite 11.0	MBV-BLIT	F.01U.393.648	License Lite base
BVMS Professional 10.1	MBV-BPRO-101	F.01U.389.492	License Professional base
BVMS Enterprise 10.1	MBV-BENT-101	F.01U.389.506	License Enterprise base
BVMS Plus 10.1	MBV-BPLU-101	F.01U.389.477	License Plus base
BVMS Viewer 10.1	MBV-BVWR-101	F.01U.389.508	License Viewer base
BVMS Lite16 10.1	MBV-BLIT-101	F.01U.389.465	License Lite base
BVMS Professional 10.0	MBV-BPRO-100	F.01U.362431	License Professional base
BVMS Enterprise 10.0	MBV-BENT-100	F.01U.362432	License Enterprise base
BVMS Plus 10.0	MBV-BPLU-100	F.01U.362445	License Plus base
BVMS Viewer 10.0	MBV-BVWR-100	F.01U.362471	License Viewer base
BVMS Lite 10.0	MBV-BLIT-100	F.01U.362455	License Lite base

9.2.2 Bosch DIVAR IP 7000 R2

Family Name	CTN	SAP#	Material description
DIVAR IP 7000 R2	DIP-7180-00N	F.01U.314.520	DIVAR IP 7000 2U w/o HDD
DIVAR IP 7000 R2	DIP-7183-4HD	F.01U.314.521	DIVAR IP 7000 2U 4x3TB
DIVAR IP 7000 R2	DIP-7183-8HD	F.01U.314.522	DIVAR IP 7000 2U 8x3TB
DIVAR IP 7000 R2	DIP-7184-4HD	F.01U.314.523	DIVAR IP 7000 2U 4x4TB
DIVAR IP 7000 R2	DIP-7184-8HD	F.01U.314.524	DIVAR IP 7000 2U 8x4TB
DIVAR IP 7000 R2	DIP-71F0-00N	F.01U.314.525	DIVAR IP 7000 3U w/o HDD
DIVAR IP 7000 R2	DIP-71F3-16HD	F.01U.314.526	DIVAR IP 7000 3U 16x3TB
DIVAR IP 7000 R2	DIP-71F4-16HD	F.01U.314.527	DIVAR IP 7000 3U 16x4TB
DIVAR IP 7000 R2	DIP-7186-8HD	F.01U.329.143	DIVAR IP 7000 2U 8x6TB
DIVAR IP 7000 R2	DIP-7188-8HD	F.01U.329.144	DIVAR IP 7000 2U 8x8TB
DIVAR IP 7000 R2	DIP-71F6-16HD	F.01U.329.145	DIVAR IP 7000 3U 16x6TB
DIVAR IP 7000 R2	DIP-71F8-16HD	F.01U.329.146	DIVAR IP 7000 3U 16x8TB
DIVAR IP 7000 R2	DIP-7184-8HD-WAG	F.01U.343.277	DIVAR IP 7000 2U 8x4TB, WAG Kit

9.2.3 Bosch DIVAR IP all-in-one 5000

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 5000	DIP-5240IG-00N	F.01U.361.821	Management Appliance w/o HDD
DIVAR IP all-in-one 5000	DIP-5244IG-4HD	F.01U.362.424	Management Appliance 4x4TB
DIVAR IP all-in-one 5000	DIP-5248IG-4HD	F.01U.362.423	Management Appliance 4x8TB
DIVAR IP all-in-one 5000	DIP-524CIG-4HD	F.01U.362.422	Management Appliance 4x12TB
DIVAR IP all-in-one 5000	DIP-5240GP-00N	F.01U.359.551	Management Appliance GPU wo HD
DIVAR IP all-in-one 5000	DIP-5244GP-4HD	F.01U.359.552	Management Appliance GPU 4x4TB
DIVAR IP all-in-one 5000	DIP-5248GP-4HD	F.01U.359.553	Management Appliance GPU 4x8TB
DIVAR IP all-in-one 5000	DIP-524CGP-4HD	F.01U.359.554	Management Appliance GPU 4x12TB

9.2.4 Bosch DIVAR IP all-in-one 7000

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 7000	DIP-7280-00N	F.01U.362.591	2U Management Appliance w/o HD
DIVAR IP all-in-one 7000	DIP-7284-8HD	F.01U.362.592	2U Management Appliance 8x4TB
DIVAR IP all-in-one 7000	DIP-7288-8HD	F.01U.362.593	2U Management Appliance 8x8TB
DIVAR IP all-in-one 7000	DIP-728C-8HD	F.01U.362.594	2U Management Appliance 8x12TB
DIVAR IP all-in-one 7000	DIP-72G0-00N	F.01U.362.595	3U Management Appliance wo HDD
DIVAR IP all-in-one 7000	DIP-72G8-16HD	F.01U.362.596	3U Management Appliance 16x8TB
DIVAR IP all-in-one 7000	DIP-72GC-16HD	F.01U.362.597	3U Management Appliance 16x12T

9.2.5 DIVAR IP all-in-one 7000 R3

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 7000	DIP-7380-00N	F.01U.385.539	Management appliance 2U without HD
DIVAR IP all-in-one 7000	DIP-7384-8HD	F.01U.385.540	Management appliance 2U 8X4TB
DIVAR IP all-in-one 7000	DIP-7388-8HD	F.01U.385.541	Management appliance 2U 8X8 TB
DIVAR IP all-in-one 7000	DIP-738C-8HD	F.01U.385.542	Management appliance 2U 8X12 TB
DIVAR IP all-in-one 7000	DIP-73G0-00N	F.01U.385.543	Management appliance 3U without HD
DIVAR IP all-in-one 7000	DIP-73G8-16HD	F.01U.385.544	Management appliance 3U 16X8TB

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 7000	DIP-73GC-16HD	F.01U.385.545	Management appliance 3U 16X12 TB

9.2.6 VJD-7513

Family Name	CTN	SAP#	Material description
VIDEOJET Decoder 7000	VJD-7513	F.01U.345.382	High-performance H.265 UHD decoder