1 Advisory Information

- **Advisory ID:** BOSCH-SA-043434-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2021-23859
    - Base Score: 9.1 (Critical)
  - CVE-2021-23860
    - Base Score: 5.0 (Medium)
  - CVE-2021-23861
    - Base Score: 6.5 (Medium)
  - CVE-2021-23862
    - Base Score: 7.2 (High)
- **Published:** 29 Nov 2021
- **Last Updated:** 29 Nov 2021

2 Summary

A recently discovered security vulnerability allows an unauthenticated attacker to cause an application to crash (Denial of Service / DoS) and for the VRM opens the possibility to send unauthenticated commands for a short time (this vulnerability is rated critical).

The VRM, DIVAR IP and BVMS with VRM are also affected by three additional vulnerabilities ranging from high to medium, allowing an authenticated remote code execution, a stored cross site scripting and access to an extended debug page.

The VIDEOJET decoder (VJD-7513 and VJD-8000) are affected by one high vulnerability (authenticated remote code execution)

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

Bosch rates these vulnerabilities with CVSSv3.1 base scores from 9.1 (Critical) to 5.0 (Medium), where the actual rating depends on the individual vulnerability and the final rating on the customer's environment.

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

3 Affected Products

- Bosch AEC <= 2.9.1.x
  - CVE-2021-23859
- Bosch APE <= 3.8.x.x
  - CVE-2021-23859
- Bosch BIS <= 4.7
  - CVE-2021-23859

- Bosch BIS <= 4.8
  - CVE-2021-23859
- Bosch BIS <= 4.9
  - CVE-2021-23859
- Bosch BVMS <= 9.0.0
  - CVE-2021-23859
  - CVE-2021-23860
  - CVE-2021-23861
  - CVE-2021-23862
- Bosch BVMS 10.0 < 10.0.2
  - CVE-2021-23859
  - CVE-2021-23860
  - CVE-2021-23861
  - CVE-2021-23862
- Bosch BVMS 10.1 < 10.1.1
  - CVE-2021-23859
  - CVE-2021-23860
  - CVE-2021-23861
  - CVE-2021-23862
- Bosch BVMS 11.0 < 11.0.0
  - CVE-2021-23859
  - CVE-2021-23860
  - CVE-2021-23861
  - CVE-2021-23862
- Bosch DIVAR IP 7000 R2 with configuration: ‘using vulnerable BVMS version’
  - CVE-2021-23859
  - CVE-2021-23860
  - CVE-2021-23861
  - CVE-2021-23862
- Bosch DIVAR IP all-in-one 5000 with configuration: ‘using vulnerable BVMS or VRM version’
  - CVE-2021-23859
  - CVE-2021-23860
  - CVE-2021-23861
  - CVE-2021-23862

- Bosch DIVAR IP all-in-one 7000 with configuration: ‘using vulnerable BVMS or VRM version’
  - CVE-2021-23859
  - CVE-2021-23860
  - CVE-2021-23861
  - CVE-2021-23862
- Bosch VJD 7513 <= 10.22.0038
  - CVE-2021-23862
- Bosch VJD 8000 <= 10.01.0036
  - CVE-2021-23862
- Bosch VRM <= 3.81
  - CVE-2021-23859
  - CVE-2021-23860
  - CVE-2021-23861
  - CVE-2021-23862
- Bosch VRM 3.82 <= 3.82.0057
  - CVE-2021-23859
  - CVE-2021-23860
  - CVE-2021-23861
  - CVE-2021-23862
- Bosch VRM 3.83 <= 3.83.0021
  - CVE-2021-23859
  - CVE-2021-23860
  - CVE-2021-23861
  - CVE-2021-23862
- Bosch VRM 4.0 <= 4.00.0070
  - CVE-2021-23859
  - CVE-2021-23860
  - CVE-2021-23861
  - CVE-2021-23862
- Bosch VRM Exporter 2.1 <= 2.10.0008
  - CVE-2021-23859

4 Solution and Mitigations

4.1 Software Updates

The recommended approach is to update the affected Bosch software to a fixed version. If an update is not possible in timely manner, users are recommended to follow the mitigation described in the following section.

4.2 Firewalling

For CVE-2021-23859 disallowing connections to Port 40080 - 40099 TCP to the software / appliance by means of a firewall prevents the attacker from accessing the vulnerable interface. If protected by a firewall the attack is limited to local signed-in users.

5 Vulnerability Details

5.1 CVE-2021-23859

CVE description: An unauthenticated attacker is able to send a special HTTP request, that causes a service to crash.

In case of a standalone VRM or BVMS with VRM installation this crash also opens the possibility to send further unauthenticated commands to the service.

On some products the interface is only local accessible lowering the CVSS base score.

For a list of modified CVSS scores, please see the official Bosch Advisory Appendix chapter

Modified CVSS Scores for CVE-2021-23859

- Problem Type:
  - CWE-703 Improper Check or Handling of Exceptional Conditions
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
  - Base Score: 9.1 (Critical)

5.2 CVE-2021-23860

CVE description: An error in a page handler of the VRM may lead to a reflected cross site scripting (XSS) in the web-based interface. To exploit this vulnerability an attack must be able to modify the HTTP header that is sent.

This issue also affects installations of the DIVAR IP and BVMS with VRM installed.

- Problem Type:
  - CWE-79 Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L
  - Base Score: 5.0 (Medium)

5.3 CVE-2021-23861

CVE description: By executing a special command, an user with administrative rights can get access to extended debug functionality on the VRM allowing an impact on integrity or availability of the installed software.

This issue also affects installations of the DIVAR IP and BVMS with VRM installed.

- Problem Type:
  - CWE-489 Active Debug Code
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H
  - Base Score: 6.5 (Medium)

5.4 CVE-2021-23862

CVE description: A crafted configuration packet sent by an authenticated administrative user can be used to execute arbitrary commands in system context.

This issue also affects installations of the VRM, DIVAR IP, BVMS with VRM installed, the VIDEOJET decoder (VJD-7513 and VJD-8000).

- Problem Type:
  - CWE-20 Improper Input Validation
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 7.2 (High)

5.5 Remark

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.

6 Additional Resources

- [1] Software Updates: https://downloadstore.boschsecurity.com
- [2] BVMS Download Area: https://downloadstore.boschsecurity.com/index.php?type=BVMS
- [3] BVMS Viewer Download Area: https://downloadstore.boschsecurity.com/index.php?type=BVMSVWR
- [4] BVMS Appliances (DIVAR IP) Download Area: https://downloadstore.boschsecurity.com/?type=DIPBVMS
- [5] VRM Download Area: https://downloadstore.boschsecurity.com/index.php?type=VRM
- [6] VJD Download Area: https://downloadstore.boschsecurity.com/index.php?type=DEC
- [7] APE Download Area: https://downloadstore.boschsecurity.com/index.php?type=APE
- [8] AEC Download Area: https://downloadstore.boschsecurity.com/index.php?type=AEC
- [9] BIS Download Area: https://downloadstore.boschsecurity.com/index.php?type=BIS

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

7 Revision History

- 29 Nov 2021: Initial Publication

8 Appendix

8.1 Modified CVSS Scores for CVE-2021-23859

On some products the affected port is protected by a firewall, lowering the CVSS score or it is only possible to cause a Denial of Service (DoS), also lowering the original score. This table shows the individual score for each product

Product	Version	CVSSv3.1 Score	CVSSv3.1 String
VRM	all	9.1 (Critical)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
BVMS with VRM	11.0	7.1 (High)	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
BVMS with VRM	10.1 and 10.0	9.1 (Critical)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
BVMS without VRM	11.0	5.5 (Medium)	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
BVMS without VRM	10.1 and 10.0	7.5 (High)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
APE	all	7.5 (High)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Divar IP	all	7.1 (High)	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
BIS	all	5.5 (Medium)	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
AEC	all	5.5 (Medium)	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

8.2 Affected Software

8.2.1 BVMS

Affected versions	Name of version to fix the vulnerability
11.0.0.1025	BVMS: BVMS11001025_Patch_SecurityIssue_350403.zip VRM: MasterInstaller_VRM_04.01.0012_64-Bit.zip
10.1.1.12	BVMS: BVMS101112_Patch_SecurityIssue_350403.zip VRM: MasterInstaller_VRM_03.83.0045_64-Bit.zip
10.0.2.13	BVMS: BVMS100213_Patch_SecurityIssue_350403.zip VRM: MasterInstaller_VRM_03.82.0069_64-Bit.zip
9.0.0.827 and older	Deprecated (please upgrade to the latest version)

BVMS Download Area

8.2.2 BVMS Viewer

Affected versions	Name of version to fix the vulnerability
11.0.0.1025	BVMS11001025_VWR_Patch_SecurityIssue_350403.zip
10.1.1.12	BVMS101112_VWR_Patch_SecurityIssue_350403.zip
10.0.2.13	BVMS100213_VWR_Patch_SecurityIssue_350403.zip
9.0.0.827 and older	Deprecated (please upgrade to the latest version)

BVMS Viewer Download Area

8.2.3 Video Recording Manager (VRM)

Affected versions	Name of version to fix the vulnerability
04.00.0070	MasterInstaller_VRM_04.01.0012_64-Bit.zip
03.83.0021	MasterInstaller_VRM_03.83.0045_64-Bit.zip
03.82.0057	MasterInstaller_VRM_03.82.0069_64-Bit.zip
03.81 and older	Deprecated (please upgrade to the latest version)

VRM Installer Download Area

8.2.4 VRM Exporter

Affected versions	Name of version to fix the vulnerability
02.10.0008	Setup_VRM_eXporter_Wizard_02.11.0014.exe (included in VRM Installer Package)

VRM Installer Download Area

8.2.5 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_BVMS11.0_MR1.zip
10.1.1.12	DIP-73_Installer_for_BVMS10.1.1_MR1.zip

BVMS Download Area

BVMS Appliances Download Area

8.2.6 Bosch DIVAR IP 7000 R2

Affected BVMS versions	Name of version to fix the vulnerability
11.0.0.1025	BVMS: BVMS11001025_Patch_SecurityIssue_350403.zip VRM: MasterInstaller_VRM_04.01.0012_64-Bit.zip
10.1.1.12	BVMS: BVMS101112_Patch_SecurityIssue_350403.zip VRM: MasterInstaller_VRM_03.83.0045_64-Bit.zip
10.0.2.13	BVMS: BVMS100213_Patch_SecurityIssue_350403.zip VRM: MasterInstaller_VRM_03.82.0069_64-Bit.zip
9.0.0 and older	Deprecated (please upgrade to the latest version)

BVMS Download Area

BVMS Appliances Download Area

8.2.7 Bosch DIVAR IP all-in-one 5000

Affected BVMS versions	Name of version to fix the vulnerability
11.0.0.1025	BVMS: BVMS11001025_Patch_SecurityIssue_350403.zip VRM: MasterInstaller_VRM_04.01.0012_64-Bit.zip
10.1.1.12	BVMS: BVMS101112_Patch_SecurityIssue_350403.zip VRM: MasterInstaller_VRM_03.83.0045_64-Bit.zip
10.0.2.13	BVMS: BVMS100213_Patch_SecurityIssue_350403.zip VRM: MasterInstaller_VRM_03.82.0069_64-Bit.zip
9.0.0	Deprecated (please upgrade to the latest version)

BVMS Download Area

BVMS Appliances Download Area

8.2.8 Bosch DIVAR IP all-in-one 7000

Affected BVMS versions	Name of version to fix the vulnerability
11.0.0.1025	BVMS: BVMS11001025_Patch_SecurityIssue_350403.zip VRM: MasterInstaller_VRM_04.01.0012_64-Bit.zip
10.1.1.12	BVMS: BVMS101112_Patch_SecurityIssue_350403.zip VRM: MasterInstaller_VRM_03.83.0045_64-Bit.zip
10.0.2.13	BVMS: BVMS100213_Patch_SecurityIssue_350403.zip VRM: MasterInstaller_VRM_03.82.0069_64-Bit.zip
9.0.0	Deprecated (please upgrade to the latest version)

BVMS Download Area

BVMS Appliances Download Area

8.2.9 Video Jet Decoder 7000

Affected versions	Name of version to fix the vulnerability
10.22.0038	VJD-7513_FW_10.23.0002.zip

VJD Installer Download Area

8.2.10 Video Jet Decoder 8000

Affected versions	Name of version to fix the vulnerability
10.01.0036	VJD-8000_FW_10.05.0001.zip

VJD Installer Download Area

8.2.11 Bosch Easy Access Controller (AEC)

Affected AEC versions	Name of version to fix the vulnerability
2.1.9.x	AEC-CVE-2021-23859.zip

AEC Download Area

8.2.12 Bosch Access Professional Edition (APE)

Affected APE versions	Name of version to fix the vulnerability
3.8.x.x (with Video functionality enabled only)	APE-CVE-2021-23859.zip

APE Download Area

8.2.13 Bosch Building Integration System (BIS)

Affected BIS versions	Name of version to fix the vulnerability
4.7	BIS-CVE-2021-23859.zip
4.8	BIS-CVE-2021-23859.zip
4.9	BIS-CVE-2021-23859.zip

BIS Download Area

8.3 Material Lists

8.3.1 BVMS

Family Name	CTN	SAP#	Material description
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

8.3.2 Video Recording Manager (VRM)

Family Name	CTN	SAP#	Material description
VRM	MVM-BVRM-016	F.01U.166.502	Base Package incl. 16 cameras single-pac

8.3.3 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

8.3.4 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

8.3.5 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

8.3.6 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

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

8.3.7 VIDEOJET decoder 7000 (VJD-7000)

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

8.3.8 VIDEOJET decoder 8000 (VJD-8000)

Family Name	CTN	SAP#	Material description
VJD-8000	VJD-8000	F.01U.313.822	VJD-8000 Decoder, H.264 bis 8MP, 60bps
VJD-8000	VJD-8000-N	F.01U.314.681	VJD-8000-N Decoder, H.264 zu 8MP, 60bps, kein TPM

8.3.9 Bosch Easy Access Controller (AEC)

Family Name	CTN	SAP#	Material description
Access Easy Controller 2.1	APC-AEC21-UPS1	F.01U.100.385	AEC2.1 Main Enclosure, PSU1
Access Easy Controller 2.1	ASL-AEC21-SWK	F.01U.100.391	Software Kit with Compact Flash Card

8.3.10 Bosch Access Professional Edition (APE)

Family Name	CTN	SAP#	Material description
Access PE	ASL-APE3P-VIDB	F.01U.298.465	Access PE - Video Activation License
Access PE	ASL-APE3P-VIDE	F.01U.298.466	Access PE - Video Expansion License

8.3.11 Bosch Building Integration System (BIS)

Family Name	CTN	SAP#	Material description
BIS - Video Engine (VIE) 4.7	BIS-FVIE-BPA47	F.01U.381.802	License for the BIS Video Engine (VIE) within BIS
BIS - Video Engine (VIE) 4.8	BIS-FVIE-BPA48	F.01U.388.192	License for the BIS Video Engine (VIE) within BIS
BIS - Video Engine (VIE) 4.9	BIS-FVIE-BPA49	F.01U.395.631	License for the BIS Video Engine (VIE) within BIS