Security Advisory: Deserialization of Untrusted Data

BVMS Mobile Video Service Vulnerability – January 2020

BOSCH-SA-885551-BT

CVE-2020-6770 (CVSS v3.1 Base Score: 10.0)

1 Overview and Management Summary

A recently discovered security vulnerability affects the BVMS Mobile Video Service (BVMS MVS). The vulnerability is exploitable via the network interface. Bosch rates this vulnerability with a CVSS v3.1 Base Score of 10.0 (Critical) and recommends customers to update the vulnerable components with fixed software versions.

The vulnerability was discovered during internal product tests.

2 Technical Details

2.1 Vulnerability Classification and Solution Approach

This vulnerability is classified as “CWE-502: Deserialization of Untrusted Data”.
CVE-2020-6770 is assigned to this vulnerability.

2.2 CVSS Rating

The CVSS v3.1 Base Score is rated at: **10.0 (Critical)**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

2.3 Impact

Attacks can be performed over the network, no physical access is required.
An attacker can leverage this vulnerability to execute arbitrary code.
The vulnerable component is the BVMS Mobile Video Service. The impacted component is the entire server system, where BVMS Mobile Video Service is running. Successful attack can have confidentiality, integrity and availability impacts.

3 Vulnerability Fix

3.1 Software Updates

The recommended approach is to update the software of affected Bosch products to a fixed version. If an update is not possible in a timely manner, the mitigation approach Firewalling can be utilized. Additional protective steps like network isolation by VLAN, IP filtering features of the devices and other technologies can be used to further decrease the exposure of vulnerable devices. A list of affected and fixed software versions is available in the “Affected Hardware” and “Affected Software” chapter of this document.

4 Mitigations and Workarounds

4.1 Firewalling (Network)

It is advised to block the inbound TCP ports 5383, 5384 and 5385. The TCP ports 5383, 5384 and 5385 must be open only for the loopback interface.

5 Affected Hardware

5.1 Bosch DIVAR IP

For Bosch DIVAR IP the following fixed firmware versions are suggested:

DIVAR IP versions	Affected versions	Name of patch to fix the vulnerability
DIVAR IP 3000	See BVMS Chapter 6.1	See BVMS Chapter 6.1
DIVAR IP 7000	See BVMS Chapter 6.1	See BVMS Chapter 6.1

6 Affected Software

6.1 BVMS Mobile Video Service

For BVMS Mobile Video Service the following patches are strongly recommended:

BVMS versions	Affected versions	Name of patch to fix the vulnerability
10.0	10.0.0.1225	BVMS10001225_Patch_SecurityIssue_243748.zip
9.0	9.0.0.827	BVMS900827_Patch_SecurityIssue_243748.zip
8.0	8.0.0.329	BVMS800329_Patch_SecurityIssue_243748.zip
7.5 and older		Not provided (please upgrade BVMS to the latest version)

BVMS Download Area

7 Direct Links

Bosch Building Technologies Security Advisory page

Bosch PSIRT

Note:
For specific software versions, which are not available in the Bosch Download Area, please contact your Bosch Support.

8 Document Change Log

2020.01.29 – Revision 1.00: Initial Release

A Appendix Bosch DIVAR IP

Family Name	CTN	SAP#	Material description
DIVAR IP 3000	DIP-3040-00N	F.01U.270.196	DIVAR IP 3000 w/o HDD
DIVAR IP 3000	DIP-3042-2HD	F.01U.270.194	DIVAR IP 3000 2x2TB
DIVAR IP 3000	DIP-3042-4HD	F.01U.270.195	DIVAR IP 3000 4x2TB
DIVAR IP 7000	DIP-7180-00N	F.01U.314.520	DIVAR IP 7000 2U w/o HDD
DIVAR IP 7000	DIP-7183-4HD	F.01U.314.521	DIVAR IP 7000 2U 4x3TB
DIVAR IP 7000	DIP-7183-8HD	F.01U.314.522	DIVAR IP 7000 2U 8x3TB
DIVAR IP 7000	DIP-7184-4HD	F.01U.314.523	DIVAR IP 7000 2U 4x4TB
DIVAR IP 7000	DIP-7184-8HD	F.01U.314.524	DIVAR IP 7000 2U 8x4TB
DIVAR IP 7000	DIP-71F0-00N	F.01U.314.525	DIVAR IP 7000 3U w/o HDD
DIVAR IP 7000	DIP-71F3-16HD	F.01U.314.526	DIVAR IP 7000 3U 16x3TB
DIVAR IP 7000	DIP-71F4-16HD	F.01U.314.527	DIVAR IP 7000 3U 16x4TB
DIVAR IP 7000	DIP-7186-8HD	F.01U.329.143	DIVAR IP 7000 2U 8x6TB
DIVAR IP 7000	DIP-7188-8HD	F.01U.329.144	DIVAR IP 7000 2U 8x8TB
DIVAR IP 7000	DIP-71F6-16HD	F.01U.329.145	DIVAR IP 7000 3U 16x6TB
DIVAR IP 7000	DIP-71F8-16HD	F.01U.329.146	DIVAR IP 7000 3U 16x8TB
DIVAR IP 7000	DIP-7184-8HD-WAG	F.01U.343.277	DIVAR IP 7000 2U 8x4TB, WAG Kit
DIVAR IP 7000	DIP-7080-00N	F.01U.282.798	DIVAR IP 7000 w/o HDD
DIVAR IP 7000	DIP-7082-8HD	F.01U.282.797	DIVAR IP 7000 8x2TB
DIVAR IP 7000	DIP-7083-8HD	F.01U.294.541	DIVAR IP 7000 8x3TB
DIVAR IP 7000	DIP-7042-4HD	F.01U.289.875	DIVAR IP 7000 4x 2TB
DIVAR IP 7000	DIP-7042-2HD	F.01U.287.694	DIVAR IP 7000 2x 2TB
DIVAR IP 7000	DIP-7040-00N	F.01U.287.695	DIVAR IP 7000 1U w/o HDD
DIVAR IP 7000	DIP-7083-8HD-WAG	F.01U.303.398	DIVAR IP 7000 2U 8x3TB WAG

B Appendix BVMS

Family name	CTN	SAP#	Material description
BVMS Professional 8.0	MBV-BPRO-80	F.01U.347.048	License Professional base
BVMS Enterprise 8.0	MBV-BENT-80	F.01U.347.049	License Enterprise base
BVMS Plus 8.0	MBV-BPLU-80	F.01U.347.064	License Plus base
BVMS Viewer 8.0	MBV-BVWR-80	F.01U.347.074	License Viewer base
BVMS Lite32 8.0	MBV-BLIT32-80	F.01U.347046	License Lite32 base
BVMS Lite64 8.0	MBV-BLIT64-80	F.01U.347047	License Lite64 base
BVMS Professional 9.0	MBV-BPRO-90	F.01U.352.132	License Professional base
BVMS Enterprise 9.0	MBV-BENT-90	F.01U.352.133	License Enterprise base
BVMS Plus 9.0	MBV-BPLU-90	F.01U.352.148	License Plus base
BVMS Viewer 9.0	MBV-BVWR-90	F.01U.352.158	License Viewer base
BVMS Lite16 9.0	MBV-BLIT16-90	F.01U.358.969	License Lite16 base
BVMS Lite32 9.0	MBV-BLIT32-90	F.01U.358.970	License Lite32 base
BVMS Lite64 9.0	MBV-BLIT64-90	F.01U.358.971	License Lite64 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

pki, BOSCH, DE, B, T, BT.ProVIRT

Digitally signed by pki, BOSCH, DE, B, T, BT.ProVIRT
Date: 2020.01.29 09:39:54 +01'00'