Security Advisory: Missing Authentication for Critical Function

Video Streaming Gateway Vulnerability – January 2020

BOSCH-SA-260625-BT

CVE-2020-6769 (CVSS v3.1 Base Score: 10.0)

1 Overview and Management Summary

A recently discovered security vulnerability affects the Bosch Video Streaming Gateway (VSG).

The vulnerability is exploitable via the network interface. An unauthorized attacker can retrieve and set arbitrary configuration data of the VSG. Bosch rates this vulnerability with a CVSS v3.1 Base Score of 10.0 (Critical) and strongly recommends customers to update vulnerable components with fixed software versions.

The vulnerability was discovered during internal security tests.

2 Technical Details

2.1 Vulnerability Classification and Solution Approach

This vulnerability is classified as “CWE-306: Missing Authentication for Critical Function”.
CVE-2020-6769 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. The complexity of the attack is low as a potential attacker does not require any specific knowledge or any specifically controlled conditions on the target environment. Successful attacks can be performed without prior authentication against the target system and without end user interaction.

The vulnerable component is the VSG service. Impacted are the VSG service itself and all cameras configured to be controlled by the VSG as well as the recording storage associated to the VSG.

Successful attacks impact the confidentiality, integrity and availability of live and recorded video data.

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, a firewall with corresponding port settings on every VSG server machine prevents attacks over the network. 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 corresponding telnet port on machines hosting the VSG service.

Each instance of the VSG service has an own dedicated port:

VSG Instance 1 uses port 8023

VSG Instance 2 uses port 8024

VSG Instance 3 uses port 8025

VSG Instance 4 uses port 8026

VSG Instance 5 uses port 8027

VSG Instance 6 uses port 8028

VSG Instance 7 uses port 8029

5 Affected Hardware

5.1 Bosch DIVAR IP with BVMS

DIVAR IP with BVMS	Vulnerable versions (until and including)	Fixed or non-vulnerable firmware versions (and later)
DIVAR IP 3000 DIVAR IP 7000 DIVAR IP all-in-one 5000	See VSG with BVMS Chapter 6.1	See VSG with BVMS Chapter 6.1

5.2 Bosch DIVAR IP 2000 and DIVAR IP 5000 (VRM/VSG only, without BVMS)

DIVAR IP without BVMS	Vulnerable versions (until and including)	Fixed or non-vulnerable firmware versions (and later)
DIVAR IP 2000	3.62.0019	3.62.0023
DIVAR IP 5000	3.80.0039	3.80.0044

DIVAR IP Download Area

By default the DIVAR IP 2000 and DIVAR IP 5000 are secured against the vulnerability described in this advisory, because the firewall settings do not allow to access the corresponding port 8023. In case the firewall settings have been changed, the vulnerability will take effect.

6 Affected Software

6.1 Bosch Video Streaming Gateway (VSG) with BVMS

For Bosch VSG in the context of BVMS the following fixed versions are suggested:

VSG versions	Corresponding BVMS version	Vulnerable versions (until and including)	Name of the patch to fix the vulnerability
6.45	9.0	6.45.08	6.45.10 (32 Bit)
6.44	9.0	6.44.0030	6.45.10 (32 Bit)
6.43	8.0	6.43.0023	6.43.0025 (32 Bit)
6.42 and older	7.5 and older	6.42.10 and older	Please update your system to a version for which a fix is provided

VSG 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 2000	DIP-2042-2HD	F.01U.270.191	DIVAR IP 2000 2x2TB
DIVAR IP 2000	DIP-2042-4HD	F.01U.270.192	DIVAR IP 2000 4x2TB
DIVAR IP 2000	DIP-2040-00N	F.01U.270.193	DIVAR IP 2000 w/o HDD
DIVAR IP 2000	DIP-2042EZ-2HD	F.01U.301.611	DIVAR IP 2000 2x2TB
DIVAR IP 2000	DIP-2042EZ-4HD	F.01U.301.612	DIVAR IP 2000 4x2TB
DIVAR IP 2000	DIP-2040EZ-00N	F.01U.301.613	DIVAR IP 2000 w/o HDD
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 5000	DIP-5042EZ-0HD	F.01U.320.208	DIVAR IP 5000 w/o HDD
DIVAR IP 5000	DIP-5042EZ-0HDX	F.01U.320.215	DIVAR IP 5000 w/o HDD w/o TPM
DIVAR IP 5000	DIP-5042EZ-1HD	F.01U.320.209	DIVAR IP 5000 1 x 2TB
DIVAR IP 5000	DIP-5042EZ-1HDX	F.01U.320.216	DIVAR IP 5000 1 x 2TB w/o TPM
DIVAR IP 5000	DIP-5042EZ-2HD	F.01U.320.210	DIVAR IP 5000 2 x 2TB
DIVAR IP 5000	DIP-5042EZ-2HDX	F.01U.320.217	DIVAR IP 5000 2 x 2TB w/o TPM
DIVAR IP 5000	DIP-5042EZ-4HD	F.01U.320.211	DIVAR IP 5000 4 x 2TB
DIVAR IP 5000	DIP-5042EZ-4HDX	F.01U.320.218	DIVAR IP 5000 4 x 2TB w/o TPM
DIVAR IP 5000	DIP-5044EZ-1HD	F.01U.320.212	DIVAR IP 5000 1 x 4TB
DIVAR IP 5000	DIP-5044EZ-1HDX	F.01U.320.219	DIVAR IP 5000 1 x 4TB w/o TPM
DIVAR IP 5000	DIP-5044EZ-2HD	F.01U.320.213	DIVAR IP 5000 2 x 4TB
DIVAR IP 5000	DIP-5044EZ-2HDX	F.01U.320.220	DIVAR IP 5000 2 x 4TB w/o TPM
DIVAR IP 5000	DIP-5044EZ-4HD	F.01U.320.214	DIVAR IP 5000 4 x 4TB
DIVAR IP 5000	DIP-5044EZ-4HDX	F.01U.320.221	DIVAR IP 5000 4 x 4TB w/o TPM
DIVAR IP 5000	DIP-5042EZ-0HD/S	F.01U.347.786	DIVAR IP 5000 w/o HDD (for Sony)
DIVAR IP 5000	DIP-5042EZ-2HD/S	F.01U.347.785	DIVAR IP 5000 2 x 2TB (for Sony)
DIVAR IP 5000	DIP-5040EZ-00N	F.01U.315.546	Storage, no HDD
DIVAR IP 5000	DIP-5040EZ-00NX	F.01U.315.548	Storage, no HDD, no TPM
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
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

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 09:38:31 +01'00'