Security Advisory: Uncontrolled Search Path Element

Bosch Software Vulnerability – March 24, 2021

BOSCH-SA-835563-BT (CVSS v3.1 Base Score: 7.8)

1 Overview and Management Summary

Multiple Bosch software applications are affected by a security vulnerability, which potentially allows an attacker to load additional code in the form of DLLs (commonly known as “DLL Hijacking” or “DLL Preloading”). This code is executed during the start of the vulnerable application and in the context of the user.

Bosch rates these vulnerabilities with a CVSS v3.1 Base Score of 7.8 (high) and recommends customers to use updated installers for (re)installations and to use updated versions of portable applications.

For BVMS and BVMS Viewer, customers are recommended to completely update the installed product to the latest version as not only the installer, but also parts of the products themselves are affected by the vulnerability.

If a software update is not provided, customers are recommended to follow the mitigations and workarounds described in this advisory.

The Bosch IP Helper vulnerability was discovered and disclosed to Bosch by the external researcher Nir Yehoshua.

The vulnerability in the Bosch Video Client Installer was discovered and disclosed to Bosch by the external researcher Eli Paz of CyberArk.

The vulnerability in the Bosch Monitor Wall Installer and Bosch Video Streaming Gateway Installer was discovered and disclosed to Bosch by the external researcher Dhiraj Mishra.

2 Technical Details

2.1 Vulnerability Classification and Solution Approach

The vulnerabilities are classified as ‘DLL Hijacking’ and affect applications and installers for Microsoft Windows. They are accordingly ranked as ‘CWE-427: Uncontrolled Search Path Element’. Possible fixes are application specific updates.

2.2 CVSS Rating

The CVSS V3.1 Base Score is rated at: 7.8 (High) CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

2.3 Impact

The vulnerability can be used to allow an attacker to supply malicious DLLs, which will be executed at runtime of the application and inherits the permission of the user starting the affected application.

Digitally signed applications will load an unsigned DLL.

3 Vulnerability Fix

3.1 Software Updates

The recommended approach is to update the affected Bosch software applications to a fixed version. If an update is not available, users are recommended to follow the mitigations and workarounds described in the following section.

Please note that for affected installers, potential exploitation is limited to the time of installation. For future (re)installations, using an updated installer or applying the workarounds outlined in this advisory is recommended.

4 Mitigations and Workarounds

4.1 Start executables from an isolated directory

Non-installed software (e.g. installers themselves and portable applications) should not be executed from directories, which are accessible by other users, or directories, where potentially malicious DLLs could be located (e.g. the default "Downloads" directory).
Installers and portable applications have no point of reference for a "known good directory/binaries". The potential impact for these kinds of software depends on the directory from which an installer or portable application is loaded ("AppDir"):

- Default "Downloads" directory: Malicious binaries may reside in a user's default Downloads folder due to prior user interaction (e.g. clicking on a malicious download link, visiting a site which manages to execute a drive-by-download) and could be loaded by an executable.

  As a mitigation, users are recommended to move executables from the Downloads directory to new separated directories not accessible by other users and only start the executables from there.
  In general, we recommend not to execute installers or other applications directly from the default Downloads directory and not to accept unsolicited download prompts in a browser.

- Directories where multiple low-privileged users have access to: If such a directory is not created by the software itself (e.g. a temporary directory during installation time), this is essentially an unprotected Installation Directory and therefore a vulnerable system configuration.

  We strongly recommend not to place executables into a directory where other low-privileged users have write permissions.
  Please note that user-created directories under C:\ (e.g. C:\MyNewFolder\) would inherit write permissions for all users and are therefore strongly discouraged.

5 Affected Software

5.1 BVMS (CVE-2020-6785)

Affected versions	Name of version to fix the vulnerability
10.1	BVMS 10.1.1 Technical Update
10.0.1	BVMS 10.0.2 Technical Update
10.0	BVMS 10.0.2 Technical Update
9.0 and older	Deprecated Please upgrade BVMS to the latest version

BVMS Download Area

5.2 BVMS Viewer (CVE-2020-6785)

Affected versions	Name of version to fix the vulnerability
10.1	BVMS Viewer 10.1.1 Technical Update
10.0.1	BVMS Viewer 10.0.2 Technical Update
10.0	BVMS Viewer 10.0.2 Technical Update
9.0 and older	Deprecated Please upgrade BVMS to the latest version

BVMS Viewer Download Area

5.3 VRM Installer (CVE-2020-6786)

Affected versions	Name of version to fix the vulnerability
3.82.0055 - 64 bit	MasterInstaller_VRM_03.82.0057_64-Bit.exe
3.81.0064 - 64 bit **3.81.0064 - 32 bit**	MasterInstaller_VRM_03.81.0067_64-Bit.exe MasterInstaller_VRM_03.81.0067_32-Bit.exe
3.71 and older	Deprecated For new installations or modifications of an existing installation please use the latest version

VRM Installer Download Area

5.4 IP Helper (CVE-2020-6771)

Affected versions	Name of version to fix the vulnerability
1.00.0008 and older	Deprecated Please use Project Assistant instead

Project Assistant Download Area

5.5 Bosch Video Client Installer (CVE-2020-6787)

Affected versions	Name of version to fix the vulnerability
1.7.6.079 and older	Deprecated Please use BVMS Viewer instead

BVMS Viewer Download Area

5.6 Bosch Configuration Manager Installer (CVE-2020-6788)

Affected versions	Name of version to fix the vulnerability
7.21.0078 and older	Setup_ConfigManager_07.30.0064.exe

Configuration Manager Download Area

5.7 Bosch Monitor Wall Installer (CVE-2020-6789)

Affected versions	Mitigations
10.00.0164 and older	Please refer to the mitigations described in this advisory.

Monitor Wall Download Area

5.8 Bosch Video Streaming Gateway Installer (CVE-2020-6790)

Affected versions	Name of patch to fix the vulnerability
6.45.10 and older	Deprecated For new installations or modifications of an existing installation please use the latest version included in BVMS

BVMS Download Area

5.9 Bosch DIVAR IP 7000 R2 (CVE-2020-6785)

Affected BVMS versions	Name of version to fix the vulnerability
10.1	BVMS 10.1.1 Technical Update and DIP-71_Patch_Installer_1.0_for_BVMS10.1.1
10.0.1	BVMS 10.1.1 Technical Update and DIP-71_Patch_Installer_1.0_for_BVMS10.1.1
10.0	BVMS 10.1.1 Technical Update and DIP-71_Patch_Installer_1.0_for_BVMS10.1.1
9.0 and older	BVMS 10.1.1 Technical Update and DIP-71_Patch_Installer_1.0_for_BVMS10.1.1

BVMS Download Area

BVMS Appliances Download Area

5.10 Bosch DIVAR IP all-in-one 5000 (CVE-2020-6785)

Affected BVMS versions	Name of version to fix the vulnerability
10.1	BVMS 10.1.1 Technical Update and DIP-52_Patch_Installer_1.0.2_for_BVMS10.1.1
10.0.1	BVMS 10.1.1 Technical Update and DIP-52_Patch_Installer_1.0.2_for_BVMS10.1.1
10.0	BVMS 10.1.1 Technical Update and DIP-52_Patch_Installer_1.0.2_for_BVMS10.1.1
9.0	BVMS 10.1.1 Technical Update and DIP-52_Patch_Installer_1.0.2_for_BVMS10.1.1

BVMS Download Area

BVMS Appliances Download Area

5.11 Bosch DIVAR IP all-in-one 7000 (CVE-2020-6785)

Affected BVMS versions	Name of version to fix the vulnerability
10.1	BVMS 10.1.1 Technical Update and DIP-72_Patch_Installer_1.0.2_for_BVMS10.1.1
10.0.1	BVMS 10.1.1 Technical Update and DIP-72_Patch_Installer_1.0.2_for_BVMS10.1.1
10.0	BVMS 10.1.1 Technical Update and DIP-72_Patch_Installer_1.0.2_for_BVMS10.1.1
9.0	BVMS 10.1.1 Technical Update and DIP-72_Patch_Installer_1.0.2_for_BVMS10.1.1

BVMS Download Area

BVMS Appliances Download Area

6 Direct Links

Software Updates:
https://downloadstore.boschsecurity.com

Security Advisory page:
https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

7 Document Changelog

2021-03-24 - Revision 1.00: Initial Publication

2021-03-30 - Revision 1.01: Version of DIP-72 Patch Installer changed from 1.0.1 to 1.0.2 (Chapter 5.11)

A Appendix BVMS

Family Name	CTN	SAP#	Material description
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

B Appendix VRM Installer

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

C Appendix Configuration Manager Installer

Family Name	CTN	SAP#	Material description
Configuration Manager	MFT-CM	F.01U.360.102	

D Appendix Monitor Wall Installer

Family Name	CTN	SAP#	Material description
Monitor Wall	MVS-MW-2D	F.01U.382.735	Monitor Wall license for two displays
Monitor Wall	MVS-MW-4D	F.01U.382.736	Monitor Wall license for four displays

E Appendix 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

F 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

G 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