Security Advisory: Buffer Overflow

Software vulnerability for Video Systems, PSIM and Access Control Systems – April 3 2019

BOSCH-2019-0403-BT

CVE-2019-6957 (CVSS v3 Base Score: 9.8)

1 Overview and management summary

A recently discovered security vulnerability affects all Bosch Video Management System (BVMS) versions 9.0 and below, DIVAR IP 2000, 3000, 5000 and 7000, Video Recording Manager (VRM), Video Streaming Gateway (VSG), Configuration Manager, Building Integration System (BIS) with Video Engine, Access Professional Edition (APE), Access Easy Controller (AEC), Bosch Video Client (BVC) and Video SDK (VSDK). The exact list of affected software versions is available in appendix A of this document.

The vulnerability potentially allows the unauthorized execution of code in the system via the network interface.

In cases where a software update is not possible, a reduction in the system's network exposure is advised. Internet-accessible installations should be firewalled, whilst additional steps like network isolation by VLAN, IP filtering features of the devices and other technologies should be used to decrease the exposure of vulnerable systems. In addition the firewall on the hosts shall be activated and set according to BVMS and BIS configuration manual. See section 4.2 Firewall on host.

2 Technical details

2.1 Vulnerability classification and solution approach

This vulnerability is classified as 'Buffer Overflow', located in the RCP+ parser of the webserver. It is accordingly ranked as "CWE-120: Buffer Copy without Checking Size of Input". The parser fix utilizes additional input and target-buffers checks.

2.2 CVSS rating

- The CVSS v3 Base Scores are rated at: 9.8 (Critical) CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
- The CVSS v3 Environmental Scores in closed network are rated at: 8.8 (High) CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A (https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A)

2.3 Impact

The vulnerability can be used to remotely execute code on the system (RCE). This would enable a potential attacker, for example, shutdown and start services or access video data. Necessary prerequisite for this attack is the network access to the webserver (HTTP / HTTPS) of the system.

3 Vulnerability fix

3.1 Software updates

The recommended approach is to update the software to a fixed version as soon as possible. Until a fixed software version is installed, the mitigation approaches firewalling, and IP filtering can be utilized. A list of affected software versions is available in appendix A of this document.

Patch and installation procedure for the latest BIS versions is available on the Bosch Download Area (Link).

4 Mitigations and workarounds

In case the referenced software patches cannot be applied, e.g. for BVMS versions 7.0 and earlier, before updating to the latest version, the following measures could mitigate the associated risk.

4.1 Firewalling (network)

It is advised that the system should not be exposed directly to the internet or other insecure networks. This includes port-forwarding, which would not protect systems adequately. Firewalling a device significantly reduces its attack surface.

Disable IP-port forwards on the external / internet router for the following services: Video Recording Manager (VRM), Video Streaming Gateway (VSG) and Mobile Video Service (MVS).

SSH can still be used. (SSH: Secure Shell, a secure communication protocol enabling encryption and mutual authentication.)

4.2 Firewall on host

For BVMS, DIP, VRM, BIS, APE, AEC and BIS, block port: 40080 TCP

For VSG, block port ranges: 8080-8086 TCP + 8443-8450 TCP

Firewalling should be applied to limit the communication to known devices.

Please see Microsoft TechNet for firewall settings: https://technet.microsoft.com

In general we recommend to open required ports only.

Configure BVMS according the following guidelines. (see configuration manual):

- https://resource.boschsecurity.com/documents/BVMS_9.0_Configuration_Manual_enUS_63356961291.pdf
- https://resource.boschsecurity.com/documents/BVMS_8.0_Configuration_Manual_enUS_35168523659.pdf
- https://resource.boschsecurity.com/documents/BoschVMS_Configuration_Manual_enUS_28154357131.pdf

4.3 Building Integration System (BIS) without Video Engine

BIS installations without Video Engine are not affected.

In case Video Engine (VSDK) was installed earlier and is not needed any more, e.g. BVMS is used instead of Video Engine, uninstall VSDK from BIS Client and delete Video Engine folder from BIS Server: C:\Mgts\ClientDeploy\Packages\Video_Engine

5 Direct links

The referenced patches (see Appendix A) are provided on the Bosch Download Area.

- Software updates: Bosch Download Area
- Bosch Building Technologies Security Advisory page
- Hardening Guide
- Bosch PSIRT Security Advisory

6 Document changelog

2019 – 04 – 03 – Revision 1.00: Initial release

Appendix A: List of affected products and fixed Software Versions

Bosch Video Management Systems (BVMS)	
Version	Fixed software version
BVMS 6.0	
BVMS 6.5	Not provided (upgrade BVMS to latest version)
BVMS 7.0	
BVMS 7.5	VRM: 3.71.0032 BVMS security patch 219829 (for BVMS 7.5)
BVMS 8.0	VRM: 3.71.0032 VSG: 6.43.0023 BVMS security patch219829 (for BVMS 8.0)
BVMS 9.0	VRM: 3.81.0048 VSG: 6.45.0008 VRM exporter: 1.20.0010 BVMS security patch 219829 (for BVMS 9.0)

DIVAR IP products	
Product family	Fixed software version
DIP 2000 / 5000	DivarIP2000_VRM-V0380.037 DivarIP5000_VRM-V0380.037
DIP 3000	See BVMS table
DIP 7000 Gen1	See BVMS table
DIP 7000 Gen2	Bosch_Appliance_BVMS_Installer_09.00.0827.0106 (Note: applicable, if system is installed from scratch or updated from BVMS version <= 8.0. For systems already running BVMS 9.0 or systems that shall remain on an earlier version, individual Hotfixes can be applied; see BVMS table).

Video Recording Manager (VRM) software	
Software	Fixed software version
Video Recording Manager (VRM)	3.71.0032 3.81.0048
Video Streaming Gateway (VSG)	6.43.0023 6.45.0008

Other software	
Software	**Fixed software version**
Configuration Manager	6.10
Video SDK (VSDK)	6.32.0099
BVC	1.7.6.079

Building Integration System (BIS)	
Version	**Fixed software version**
BIS 2.2 - 4.4	Not provided (upgrade BIS to latest version if Video Engine is used)
BIS 4.5, 4.6 and 4.6.1	BIS security patch 4.6.9928.0 VSDK 6.32.0099 (see Patch Procedure on Download Store)

Access Professional Edition (APE)	
Software	**Fixed software version**
Earlier Versions of APE	Not provided (upgrade APE to latest version)
APE 3.0 to APE 3.7 (only affected if Third-Party component VSDK is installed; see Control Panel\Programs\Programs and Features\Bosch VideoSDKxx.xx.xxxx)	Install Patch Setup 3.7.2.3 VSDK 6.32.0099

Access Easy Controller (AEC)	
Software	**Fixed software version**
Earlier Versions of AEC	Not provided (upgrade AEC to latest version)
Access Easy Controller 2.1.9.0 (AEC)	AEC Firmware AEC2.1 Video plugins version 6.32.0099 - 2.0.0.4
Access Easy Controller 2.1.9.1 (AEC)	AEC Firmware AEC2.1 Video plugins version 6.32.0099 - 2.0.0.4
Access Easy Controller 2.1.9.3 (AEC)	AEC Firmware AEC2.1 Video plugins version 6.32.0099 - 2.0.0.4
Access Easy Controller 2.1.8.5 (AEC)	AEC Firmware AEC2.1 Video plugins version 6.32.0099 - 2.0.0.4

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

Digitally signed by pki, BOSCH, DE, B, T, BT.ProVIRT
Date: 2019.04.03 10:00:54 +02'00'