BOSCH

Kritische Schwachstelle in Bosch Video Software (CVE-2019-8951, -8952, -6957, -6958 -11684)

Register: (BVMS, DIVAR-IP, VRM, VSDK, BVC, CM)

TECHNISCHE INFORMATION 2242/2019

ÄND.-KLASSE		KRITERIUM
I	☐	Die Änderung muss sofort eingebracht werden.
II	☒	Die Änderung muss bei in Betrieb befindlichen Anlagen
III	☐	Änderungen im Fehlerfall und bei Neuinstallationen einbringen
KEINE	☐	

ALLGEMEIN

Diese TI umfasst fünf Security Advisories: CVE-2019-8951, CVE-2019-8952, CVE-2019-6957, CVE-2019-6958, CVE-2019-11684
Veröffentlichte Details finden Sie hier auf unserer Website mit **Security Advisories**:
https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

ANZAHL DER BETROFFENEN SYSTEME: **In Summe ca. 2.300 Installations-Standorte** (siehe Aufstellung am Ende)
Erforderliche Maßnahmen gemäß Änderungsklasse 2: ca. 550 Systeme

☒ **HARDWARE**

BEZEICHNUNG	CTN	SAP-NR	VERTRIEBSZEITRAUM
DIVAR IP 2000 (iSCSI-Speicher mit optionalem VRM)			
DIVAR IP 2000 2x2TB	DIP-2042-2HD	F.01U.270.191	09.2013 bis 01.2015
DIVAR IP 2000 4x2TB	DIP-2042-4HD	F.01U.270.192	09.2013 bis 01.2015
DIVAR IP 2000 w/o HDD	DIP-2040-00N	F.01U.270.193	09.2013 bis 01.2015
DIVAR IP 2000 EZ 2x2TB	DIP-2042EZ-2HD	F.01U.301.611	01.2015 bis 11.2016
DIVAR IP 2000 EZ 2x4TB	DIP-2042EZ-4HD	F.01U.301.612	01.2015 bis 11.2016
DIVAR IP 5000 (iSCSI-Speicher mit optionalem VRM)			
DIVAR IP 5000 w/o HDD	DIP-5042EZ-0HD	F.01U.320.208	05.2016 bis 06.2019
DIVAR IP 5000 1 x 2TB	DIP-5042EZ-1HD	F.01U.320.209	05.2016 bis 06.2019
DIVAR IP 5000 2 x 2TB	DIP-5042EZ-2HD	F.01U.320.210	05.2016 bis 06.2019
DIVAR IP 5000 4 x 2TB	DIP-5042EZ-4HD	F.01U.320.211	05.2016 bis 06.2019
DIVAR IP 5000 1 x 4TB	DIP-5044EZ-1HD	F.01U.320.212	05.2016 bis 06.2019
DIVAR IP 5000 2 x 4TB	DIP-5044EZ-2HD	F.01U.320.213	05.2016 bis 06.2019
DIVAR IP 5000 4 x 4TB	DIP-5044EZ-4HD	F.01U.320.214	05.2016 bis 06.2019
DIVAR IP 3000 (BVMS, iSCSI-Speicher, VRM)			
DIVAR IP 3000 2x2TB	DIP-3042-2HD	F.01U.270.194	07.2013 bis 01.2019
DIVAR IP 3000 4x2TB	DIP-3042-4HD	F.01U.270.195	07.2013 bis 01.2019
DIVAR IP 3000 w/o HDD	DIP-3040-00N	F.01U.270.196	07.2013 bis 01.2019
DIVAR IP 6000 (R1) (iSCSI-Speicher mit optionalem VRM)			
DIVAR IP 6000 4x2TB	DIP-6042-4HD	F.01U.282.799	09.2013 bis 02.2016
DIVAR IP 6000 8x2TB	DIP-6082-8HD	F.01U.282.801	09.2013 bis 02.2016
DIVAR IP 6000 1U 4x3TB	DIP-6043-4HD	F.01U.294.509	09.2013 bis 02.2016
DIVAR IP 6000 2U 8x3TB	DIP-6083-8HD	F.01U.294.540	05.2015 bis 02.2016
DIVAR IP 6000 1U w/o HDD	DIP-6040-00N	F.01U.282.800	02.2014 bis 02.2016
DIVAR IP 6000 2U w/o HDD	DIP-6080-00N	F.01U.282.802	02.2014 bis 02.2016

BEZEICHNUNG	CTN	SAP-NR	VERTRIEBSZEITRAUM
DIVAR IP 6000 (R2) (iSCSI-Speicher mit optionalem VRM)			
DIVAR IP 6000 2U w/o HDD (R2)	DIP-6180-00N	F.01U.308.406	04.2016 bis 12.2019
DIVAR IP 6000 2U 4x3TB (R2)	DIP-6183-4HD	F.01U.308.452	04.2016 bis 12.2019
DIVAR IP 6000 2U 8x3TB (R2)	DIP-6183-8HD	F.01U.308.453	04.2016 bis 12.2019
DIVAR IP 6000 2U 4x4TB (R2)	DIP-6184-4HD	F.01U.308.454	04.2016 bis 12.2019
DIVAR IP 6000 2U 8x4TB (R2)	DIP-6184-8HD	F.01U.308.455	04.2016 bis 12.2019
DIVAR IP 6000 3U w/o HDD (R2)	DIP-61F0-00N	F.01U.308.456	04.2016 bis 12.2019
DIVAR IP 6000 3U 16x3TB (R2)	DIP-61F3-16HD	F.01U.308.457	04.2016 bis 12.2019
DIVAR IP 6000 3U 16x4TB (R2)	DIP-61F4-16HD	F.01U.308.458	04.2016 bis 12.2019
DIVAR IP 6000 2U 6x8TB (R2)	DIP-6186-8HD	F.01U.329.139	06.2017 bis 12.2019
DIVAR IP 6000 2U 8x8TB (R2)	DIP-6188-8HD	F.01U.329.140	06.2017 bis 12.2019
DIVAR IP 6000 2U 16x6TB (R2)	DIP-61F6-16HD	F.01U.329.141	06.2017 bis 12.2019
DIVAR IP 6000 2U 16x8TB (R2)	DIP-61F8-16HD	F.01U.329.142	06.2017 bis 12.2019
DIVAR IP 7000 (R1)			
DIVAR IP 7000 1U 4x 2TB	DIP-7042-4HD	F.01U.289.875	09.2013 bis 02.2016
DIVAR IP 7000 1U 2x 2TB	DIP-7042-2HD	F.01U.287.694	09.2013 bis 02.2016
DIVAR IP 7000 8x2TB	DIP-7082-8HD	F.01U.282.797	09.2013 bis 02.2016
DIVAR IP 7000 2U 8x3TB	DIP-7083-8HD	F.01U.294.541	09.2013 bis 02.2016
DIVAR IP 7000 1U w/o HDD	DIP-7040-00N	F.01U.287.695	09.2013 bis 02.2016
DIVAR IP 7000 2U w/o HDD	DIP-7080-00N	F.01U.282.798	02.2014 bis 02.2016
DIVAR IP 7000 (R2)			
DIVAR IP 7000 2U w/o HDD (R2)	DIP-7180-00N	F.01U.314.520	04.2016 bis 12.2019
DIVAR IP 7000 2U 4x3TB (R2)	DIP-7183-4HD	F.01U.314.521	04.2016 bis 12.2019
DIVAR IP 7000 2U 8x3TB (R2)	DIP-7183-8HD	F.01U.314.522	04.2016 bis 12.2019
DIVAR IP 7000 2U 4x4TB (R2)	DIP-7184-4HD	F.01U.314.523	04.2016 bis 12.2019
DIVAR IP 7000 2U 8x4TB (R2)	DIP-7184-8HD	F.01U.314.524	04.2016 bis 12.2019
DIVAR IP 7000 3U w/o HDD (R2)	DIP-71F0-00N	F.01U.314.525	04.2016 bis 12.2019
DIVAR IP 7000 3U 16x3TB (R2)	DIP-71F3-16HD	F.01U.314.526	04.2016 bis 12.2019
DIVAR IP 7000 3U 16x4TB (R2)	DIP-71F4-16HD	F.01U.314.527	04.2016 bis 12.2019
DIVAR IP 7000 2U 6x8TB (R2)	DIP-7186-8HD	F.01U.329.143	06.2017 bis 12.2019
DIVAR IP 7000 2U 8x8TB (R2)	DIP-7188-8HD	F.01U.329.144	06.2017 bis 12.2019
DIVAR IP 7000 2U 16x6TB (R2)	DIP-71F6-16HD	F.01U.329.145	06.2017 bis 12.2019
DIVAR IP 7000 2U 16x8TB (R2)	DIP-71F8-16HD	F.01U.329.146	06.2017 bis 12.2019

☒ SOFTWARE

BEZEICHNUNG	BEMERKUNG	VERSION ALT	VERSION NEU (oder höher)
BVMS (jeweils in den Versionen: Demo, Lite 32, Lite 64, Professional, Enterprise und PLUS)			
BVMS 7.0 und kleiner	Wird nicht gepatched	Upgrade auf mind. BVMS 7.5 erforderlich Upgrade auf BVMS 9.0 empfohlen	
BVMS 7.5	VRM	ältere Versionen	3.71.0034
	BVMS Security Patch	----	219829
BVMS 8.0	VRM	Älter als 3.71.0034	3.71.0034
	VSG	Älter als 6.43.002	6.43.0023
	BVMS Security Patch	----	219829
BVMS 9.0	VRM	Älter als 3.81.0050	3.81.0050
	VSG	Älter als 6.45.0008	6.45.0008
	VRM exporter	Älter als 1.20.0010	1.20.0010
	BVMS Security Patch	----	219829

BEZEICHNUNG	BEMERKUNG	VERSION ALT	VERSION NEU
Image-Versionen für DIVAR IP			
DIVAR IP 2000	VRM-Version für Divar IP 2000	Älter als VRM-V0362.019	VRM-V0362.019
DIVAR IP 5000	VRM-Version für Divar IP 5000	Älter als VRM-V0380.039	VRM-V0380.039
VRM-Versionen auf verschiedener Hardware			
DIVAR IP 3000		Siehe BVMS Version bis 8.0	
DIVAR IP 7000 (R1)		Siehe BVMS Version bis 8.0	
DIVAR IP 7000 (R2)	BVMS 5.0 bis 7.5	Verwenden Sie die Vorgaben / Hotfixes gemäß o.g. BVMS Versionen	
DIVAR IP 7000 (R2)	BVMS 8.0 und 9.0	Verwenden Sie bei einem Update von 8.0 auf 9.0 oder einer 9.0 Neuinstallation den *Bosch_Appliance_BVMS_Installer_09.00.0827.0106*	
Weitere Software			
Configuration Manager		Älter als 6.10	6.10
Video SDK (VSDK)		Älter als 6.32.0099	6.32.0099
BVC		Älter als 1.7.6.079	1.7.6.079

BESCHREIBUNG:

CVE-2019-11684 „Unauthenticated Certificate Access“ (CVSS-Bewertung: 9,9 - Kritisch)
Die Sicherheitslücke liegt im Video Recording Manager (VRM) ab Version 3.70.
Diese Sicherheitsanfälligkeit wird als „Unsachgemäße Zugriffssteuerung" klassifiziert. Der betroffene RCP+ -Server der VRM-Komponente ermöglicht den willkürlichen und nicht authentifizierten Zugriff auf Teilebereiche der Windows-Zertifikate.

CVE-2019-6957 "Buffer Overflow" (CVSS-Bewertung: 9,8 - Kritisch)
Die Schwachstelle betrifft alle Bosch Video Management System (BVMS) bis einschließlich Version 9.0, DIVAR IP Systemen (DIP), Video Recording Manager (VRM), Video-Streaming-Gateway (VSG), Configuration Manager (CM), Bosch Video Client (BVC) und Video SDK (VSDK).
Diese Sicherheitslücke wird als "Pufferüberlauf" eingestuft, der sich im RCP + -Parser des Webservers befindet.

CVE-2019-6958 „Improper Access Control“ (CVSS-Bewertung: 9,8 - Kritisch)
Diese Schwachstelle ermöglicht über den RCP+ -Netzwerkanschluss den Zugriff ohne Authentifizierung.
Diese Sicherheitslücke wird als wird als „unzulässige Zugriffskontrolle“ eingestuft.

CVE-2019-8951 „Open Redirect“ (CVSS-Bewertung: 6,1 - Mittel)
Die Schwachstelle liegt in der Video Recording Manager (VRM) seit Version 3.10. Die Sicherheitslücke ist in Version 3.80 oder höher behoben. Vorgängerversionen gelten als nicht betroffen.
Diese Sicherheitslücke befindet sich im Webserver und wird als eine URL-Weiterleitung an eine nicht vertrauenswürdige Site „Open Redirect“ eingestuft.

CVE-2019-8952 „Path Traversal“ (CVSS-Bewertung: 4,9 - Mittel)
Die Schwachstelle betrifft den Video Recording Manager (VRM) der auf den DIVAR IP Systemen (DIP) und in Zusammenhang mit allen Bosch Video Management Systemen (BVMS) bis einschließlich Version 9.0 betrieben wird.
Diese Sicherheitslücke wird als „Path Traversal“ klassifiziert und befindet sich im Webserver.

AUSWIRKUNGEN (Kurzfassung):

CVE-2019-11684 „Unauthenticated Certificate Access”
Die Sicherheitslücke ermöglicht Zugriff auf Zertifikate im Windows Zertifikatsspeicher. Dabei können vorhandene Zertifikate geändert oder gelöscht, sowie neue Zertifikate hinzugefügt werden. Der Zugriff ist nach den aktuellen Erkenntnissen auf den Bereich „Lokales System“ beschränkt. Im ungünstigsten Fall kann ein Änderungsversuch zu einem vorübergehenden Einfrieren des VRM und der zugehörigen Komponenten führen.
Der „Attack Vector“ kann über die Ports 80 (http) und 443 (https) auf Netzwerkebene ausgeführt werden. Die Änderung von SSL-Zertifikaten für die Verschlüsselungsaufzeichnung kann dazu führen, dass Videodaten aufgezeichnet werden, auf die der angegebene Bediener keinen Zugriff hat. Somit können, nach einer Manipulation der Zertifikate aufgezeichnete Videodaten verloren gehen.

CVE-2019-6957 "Buffer Overflow"
Die Sicherheitslücke kann zum Remote-Ausführen von Codes auf dem System (RCE) verwendet werden. Dies würde einem potenziellen Angreifer ermöglichen, beispielsweise Dienste herunterzufahren und zu starten oder auf Videodaten zuzugreifen. Voraussetzung für diesen Angriff ist der Netzwerkzugriff auf den Webserver (HTTP / HTTPS) des Systems.

CVE-2019-6958 „Improper Access Control“
Diese Sicherheitslücke kann es einem potenziellen Angreifer ermöglichen, Videodaten zu Lesen oder zu Löschen.

CVE-2019-8951 „Open Redirect“
Die Schwachstelle kann es einem potenziellen Angreifer ermöglichen, die Benutzeranforderung im Webbrowser erfolgreich an eine böswillige Website umzuleiten. Eine notwendige Voraussetzung für diesen Angriff ist ein mit dem Internet verbundenes System.

CVE-2019-8952 „Path Traversal“
Die Sicherheitslücke kann dazu verwendet werden, das Dateisystem remote zu durchsuchen, um auf Dateien oder Verzeichnisse zuzugreifen, die sich außerhalb des eingeschränkten Verzeichnisbereichs befinden. Eine notwendige Voraussetzung für diesen Angriff ist der Netzwerkzugriff auf den Webserver (HTTP / HTTPS) des Geräts und gültige Anmeldedaten.

ABHILFE/ MAßNAHME:

Bei allen genannten Security Advisories wird die Schwachstelle mit einem Update auf eine fehlerbereinigte SW/FW-Version behoben.
Die referenzierten Patches werden in der *Bosch Download Area* zur Verfügung gestellt: Bosch Download Store
Alternativ können diese in gesammelter Form vom Video-Portalraum heruntergeladen werden: → **LINK**
Hinweis: Die hier erhältlichen FW- und SW-Stände stellen den aktuellen Stand (zum 08.04.19) dar. Somit kann jeder ohne wenig Aufwand sich das „Mindest-Paket“ herunterladen. Diese Daten werden hier nicht gepflegt und Ende des Jahres wieder gelöscht.

Bitte beachten Sie, dass ebenfalls die FW für Kameras, Encoder, Decoder auf die jeweils letzte Version (CPP abhängig) aktualisiert werden muss. Diese Information finden Sie in Bosch Connect unter BT-SC: Product Management → **FIRMWARE**

Solange kein Update erfolgt ist, sind Maßnahmen zur Risikominimierung zu ergreifen:

1.0 Allgemein - Netzwerk
Deaktivieren Sie die Portfreigabe/Portweiterleitung (NAT)auf dem Internet-Router für die folgenden Dienste:
Video Recording Manager (VRM), Video Streaming Gateway (VSG) und Mobile Video Service (MVS). SSH (Security Shell) kann weiterhin verwendet werden.

2.0 Firewall (Host)
Für BVMS, DIVAR IP und VRM: Blockieren Sie Port 40080 TCP
Für den VSG: Blockieren Sie die Ports 8080-8086 TCP + 8443-8450 TCP
Firewall sollte angewendet werden, um die Kommunikation mit bekannten Geräten zu beschränken.

3.0 Informationen zu den Firewall-Einstellungen finden Sie unter Microsoft TechNet: https://technet.microsoft.com

4.0 Im Allgemeinen empfehlen wir, nur die erforderlichen Ports zu öffnen.
Konfigurieren Sie BVMS gemäß den folgenden Richtlinien. (siehe Konfigurationshandbuch):
- ► http://resource.boschsecurity.com/documents/BVMS_9.0_Configuration_Manual_enUS_63356961291.pdf
- ► http://resource.boschsecurity.com/documents/BVMS_8.0_Configuration_Manual_enUS_35168523659.pdf
- ► http://resource.boschsecurity.com/documents/BoschVMS_Configuration_Manual_enUS_28154357131.pdf

Sollte ein Software Update nicht durchführbar sein, so empfehlen wir die Sichtbarkeit des Systems im Netzwerk zu reduzieren und das betroffene Videosystem durch Firewall-Regeln weitgehend unerreichbar zu machen. Die Firewall Einstellungen sind entsprechend der Empfehlungen durchzuführen.

VORAUSSETZUNGEN ZUM SYSTEM-UPGRADE:

Grundsätzlich empfehlen wir ein Upgrade auf die aktuelle BVMS Version (9.0), weil diese Version den höchsten Sicherheitsstandard hat.
Voraussetzung für ein Upgrade ist ein gültiges SMA. Dieses ist u.a. im Effilink Software Assurance Vertrag (ESA) enthalten.
Hierbei muss das „**Maintenance expiration date**“ nach dem **17.08.2018** liegen. Diese Information finden Sie im Activation Manager (online) oder im Maintenance Report des jeweiligen BVMS-Systems.

Folgende ältere Versionen werden zum Update auf BVMS 9.0 am häufigsten erwartet:

Farb-Definition:
Text in rot = kann definitiv nicht mehr bei der referenzierten BVMS 9.0 verwendet werden
Text in grün = kann bei der referenzierten BVMS 9.0 verwendet werden
Text in blau = kann bedingt im Einzelfall bei der referenzierten BVMS 9.0 verwendet werden, Prüfung erforderlich!

BVMS 4.5.5 auf BVMS 9.0

	Betroffene HW	Für BVMS 4.5.5 freigegeben	Für BVMS 9.0 erforderlich	Bemerkung / Hinweise
1	Workstation / BVMS-Client	Windows XP Windows 7	Windows 10 (1809)	Wechsel von 32 Bit auf 64 Bit System
2	Workstation / BVMS-Client	Intel Core 2 Duo Min. 500MB-HDD	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8 GB RAM	Auf Ausgänge der Grafikkarten achten
3	Server / VRM Management	Windows Storage Server 2008 R2	WS Server 2012 R2 (64-bit)	Empfohlen: WS Server 2016
4	Server / VRM Management	Intel Core 2 Duo Min. 500MB-HDD, 4 GB RAM	Intel Xeon E5-2620v3 (2.4 GHz, 6-core, 15MB), min. 1GB-HDD, 8 GB RAM	

BVMS 5.0 auf BVMS 9.0

	Betroffene HW	Für BVMS 5.0 freigegeben	Für BVMS 9.0 erforderlich	Bemerkung / Hinweise
1	Workstation / BVMS-Client	Windows 7 Windows 8.1 64 Bit	Windows 10 (1809)	Wechsel von 32 Bit auf 64 Bit System
2	Workstation / BVMS-Client	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Auf Ausgänge der Grafikkarten achten
3	Server / VRM Management	Windows Storage Server 2008 R2 Windows Storage Server 2012 R2	WS Server 2012 R2 (64-bit)	Empfohlen: WS Server 2016
4	Server / Management / VRM / MVS	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Intel Xeon E5-2620v3 (2.4 GHz, 6-core, 15MB), min. 1GB-HDD, 8 GB RAM	HW (IC i7) kann bei Anwendungen bis 64 Kanälen ausreichen. → Bitte Prüfen!

BVMS 5.5.5 auf BVMS 9.0

	Betroffene HW	Für BVMS 5.5.5 freigegeben	Für BVMS 9.0 erforderlich	Bemerkung / Hinweise
1	Workstation / BVMS-Client	Windows 7 Windows 8.1 64 Bit	Windows 10 (1809)	Wechsel von 32 Bit auf 64 Bit System
2	Workstation / BVMS-Client	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Auf Ausgänge der Grafikkarten achten
3	Server / VRM Management	Windows Storage Server 2008 R2 Windows Storage Server 2012 R2	WS Server 2012 R2 (64-bit)	Empfohlen: WS Server 2016
4	Server / Management / VRM / MVS	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Intel Xeon E5-2620v3 (2.4 GHz, 6-core, 15MB), min. 1GB-HDD, 8 GB RAM	HW (IC i7) kann bei Anwendungen bis 64 Kanälen ausreichen. → Bitte Prüfen!

BVMS 6.0 auf BVMS 9.0

	Betroffene HW	Für BVMS 6.0 freigegeben	Für BVMS 9.0 erforderlich	Bemerkung / Hinweise
1	Workstation / BVMS-Client	Windows 7 Windows 8.1 64 Bit	Windows 10 (1809)	Wechsel von 32 Bit auf 64 Bit System
2	Workstation / BVMS-Client	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Auf Ausgänge der Grafikkarten achten
3	Server / VRM Management	Windows Storage Server 2008 R2 Windows Storage Server 2012 R2	WS Server 2012 R2 (64-bit)	Empfohlen: WS Server 2016
4	Server / Management / VRM / MVS	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Intel Xeon E5-2620v3 (2.4 GHz, 6-core, 15MB), min. 1GB-HDD, 8 GB RAM	HW (IC i7) kann bei Anwendungen bis 64 Kanälen ausreichen. → Bitte Prüfen!

BVMS 6.5 auf BVMS 9.0

	Betroffene HW	Für BVMS 6.5 freigegeben	Für BVMS 9.0 erforderlich	Bemerkung / Hinweise
1	Workstation / BVMS-Client	Windows 7 Windows 8.1 64 Bit	Windows 10 (1809)	Wechsel von 32 Bit auf 64 Bit System
2	Workstation / BVMS-Client	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Auf Ausgänge der Grafikkarten achten
3	Server / VRM Management	Windows Storage Server 2008 R2 Windows Storage Server 2012 R2	WS Server 2012 R2 (64-bit)	Empfohlen: WS Server 2016
4	Server / Management / VRM / MVS	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Intel Xeon E5-2620v3 (2.4 GHz, 6-core, 15MB), min. 1GB-HDD, 8 GB RAM	HW (IC i7) kann bei Anwendungen bis 64 Kanälen ausreichen. → Bitte Prüfen!

BVMS 7.0 auf BVMS 9.0

	Betroffene HW	Für BVMS 7.0 freigegeben	Für BVMS 9.0 erforderlich	Bemerkung / Hinweise
1	Workstation / BVMS-Client	Windows 8.1 64 Bit Windows 10 (1607) anniversary	Windows 10 (1809)	Wechsel von 32 Bit auf 64 Bit System
2	Workstation / BVMS-Client	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Auf Ausgänge der Grafikkarten achten
3	Server / VRM Management	Windows Storage Server 2008 R2 Windows Storage Server 2012 R2	WS Server 2012 R2 (64-bit)	Empfohlen: WS Server 2016
4	Server / Management / VRM / MVS	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	Intel Xeon E5-2620v3 (2.4 GHz, 6-core, 15MB), min. 1GB-HDD, 8 GB RAM	HW (IC i7) kann bei Anwendungen bis 64 Kanälen ausreichen. → Bitte Prüfen!

Um die Sicherheitsanforderungen dieser TI zu erfüllen, ist es ausreichend, BVMS auf Version 7.5 upzudaten. Dennoch empfehlen wir gleich auf BVMS 9.0 zu gehen, weil in dieser Version auch andere mögliche Fehlererscheinungen behoben sind. Auch ist zu beachten, dass der Servicezeitraum der aktuellen BVMS 9.0 zu einem späteren Zeitpunkt als bei BVMS 7.5 abläuft (End of Service).

Zum Vergleich die Mindest-Voraussetzungen für BVMS 7.5.

	Betroffene HW	Für BVMS 7.5 freigegeben	Freigegeben seit BVMS-Version ...	Bemerkungen
1	Workstation / BVMS-Client	Windows 8.1 64 Bit Windows 10 (1607) anniversary	ab BVMS 5.0 ab BVMS 7.5	Windows 8.1 64 Bit end of service seit 9.1.18 (regulärer Support), ab 10.1.23 (erweiterter Support)
2	Workstation / BVMS-Client	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	ab BVMS 5.0	
3	Server / VRM Management	Windows Storage Server 2008 R2 Windows Storage Server 2012 R2	ab BVMS 4.5 ab BVMS 5.0	Windows Server 2008 R2 end of service seit 13.1.15 (regulärer Support), ab 14.1.20 (erweiterter Support)
4	Server / Management / VRM / MVS	Intel Core i7 4770 3.4 GHz bis 3.9 GHz Min. 3 GB-HDD, 8GB RAM	ab BVMS 5.0	

BESONDERE BETRACHTUNG:

Systeme, deren Hardware- und Betriebssystem-Spezifikation vor den Release der BVMS 4.5.5 lagen, wurde ich nicht betrachtet. Dieses muss jedoch in die Einzelbetrachtung, wenn BVMS 4.5.5 bereits über Upgrades erreicht wurde, einbezogen werden.

HINWEISE:

Die Kritikalität hängt von der Netzwerkumgebung ab, in welcher sich das Videosystem befindet. Systeme, die direkt mit dem Internet verbunden sind, unterliegen einem höheren Risiko von einem Angriff betroffen zu werden, als ein System in einem geschützten Netzwerksegment hinter einer Firewall.

Stellen Sie sicher, dass alle Videosysteme, die über eine Internetverbindung verfügen gepatched oder upgedatet wurden.
Anderen Falls kann kein Support mehr geleistet werden!

Wichtig: Weiterführende Informationen zu dieser Schwachstelle finden Sie im WiKi des BT-IE Security Operations Center (SOC): https://inside-docupedia.bosch.com/confluence/display/IESOC/.

ZEITAUFWÄNDE:

Weil hier keine einheitliche „Pauschalanlage“ für die Planzeit verwendet werden kann, haben wir nachfolgend die Aufwände je Hardware beziffert. Diese muss dann nach Anlagen-Konstellation addiert werden.
Die Zeiten sind gemittelt und können im Einzelfall je nach Komplexität der Anlage nach oben und unten abweichen.

Hardware	SW-Patch	SW-Update	Versions-Upgrade	Bemerkung	Gesamt-Zeit
DIVAR IP 2000 / 5000	----------	VRM-Update 30 Minuten	----------	Alle Updates im neuen Image enthalten	30 Minuten
DIVAR IP 3000	BVMS-Patch 15 Minuten	VRM-Update 30 Minuten	BVMS 7.5 ... 8.0 90 Minuten	BVMS-Upgrade inkl. Config sichern, System-Prüfung, etc.	135 Minuten
DIVAR IP 6000 (R1/2)	----------	VRM-Update 45 Minuten	----------	Daten sichern / einspielen, Anlage überprüfen, etc.	45 Minuten
DIVAR IP 7000 (R1/2)	BVMS-Patch 15 Minuten	VRM-Update 30 Minuten	BVMS 7.5 ... 9.0 90 Minuten	BVMS-Upgrade inkl. Config sichern, System-Prüfung, etc.	135 Minuten
VRM-Server (Stand Alone)	----------	VRM-Update 45 Minuten	----------	Daten sichern / einspielen, Anlage überprüfen, etc.	45 Minuten
BVMS-Server	BVMS-Patch 15 Minuten	----------	BVMS 7.5 ... 9.0 90 Minuten	BVMS-Upgrade inkl. Config sichern, System-Prüfung, etc.	105 Minuten
BVMS-Client (Workstation)	BVMS-Patch 15 Minuten	----------	BVMS 7.5 ... 9.0 125 Minuten.	Funktionsupdates (Windows) sind parallel notwendig	140 Minuten
Kamera, Encoder und Decoder	----------	----------	FW-Update 1 Minute	Hier kann ein Update parallel erfolgen.	1 Minute

Zusatzbemerkungen zu den Zeiten:
Je nach SW/FW-Version kann es erforderlich sein, dass auf Zwischenversionen upgedatet werden muß, bevor die finale Version verwendet werden kann. Diese Zeiten sind hier bereits berücksichtigt.

ANZAHL BETROFFENER SYSTEME (gerundet):

DIVAR IP 2000 / 5000	390 Stück
DIVAR IP 3000	1.500 Stück
DIVAR IP 6000 (R1/R2)	490 Stück
DIVAR IP 7000 (R1/R2)	590 Stück
BVMS-Server	100 Stück
BVMS-Client (WS)	300 Stück
VRM-Server	100 Stück

ANLAGEN:

- Advisory CVE-2019-6951.pdf
- Advisory CVE-2019-6952.pdf
- Advisory CVE-2019-6957.pdf
- Advisory CVE-2019-6958.pdf
- Advisory CVE-2019-11684.pdf

HINWEIS:

Die Kunden / Projekte wurden nach Relevants und Dringlichkeit gefiltert und entsprechend der TI mit Änderungsklasse 1 (2241/2019) oder Änderungsklasse 2 (2242/2019) zugeordnet. Die zugehörigen Bocams-Tickets werden von der ZSL Magdeburg erstellt und zeitnah ausgegeben. Kunden ohne vertragliche Verbindlichkeiten oder Gewährleistungsanspruch werden separat angeschrieben.

Mit freundlichen Grüßen
Bosch Sicherheitssysteme GmbH

BT-IE/PRM3 Reutter

BT-IE/PRM1 Konopka