Kritische Schwachstelle in Bosch IP-Kameras (CVE-2018-19036)

Register: (Videosysteme/Videokameras)

TECHNISCHE INFORMATION 2208/2018

ÄND.-KLASSE		KRITERIUM
I	☐	Die Änderung muss sofort eingebracht werden.
II	☒	Die Änderung muss bei in Betrieb befindlichen Anlagen im Rahmen der nächsten Inspektion/ Wartung gemäß vereinbarten Serviceklassen eingebracht werden. Umsetzung bis spätestens 30. Juni 2019.
III	☐	Änderungen im Fehlerfall und bei Neuinstallationen einbringen
KEINE	☐	

ANZAHL DER BETROFFENEN SYSTEME/ ANLAGEN/ MELDER: ca. 4700 Installationen

☒ **HARDWARE**

BEZEICHNUNG	CTN	SAP-NR	FERTIGUNGSZEITRAUM
Beachten Sie die Liste der betroffenen Hardware im Anhang A.			

☒ **SOFTWARE**

BEZEICHNUNG	CTN	SAP-NR	VERSION ALT	VERSION NEU
Alle Versionen ab 6.32	-	-	-	6.44.0027
Alle Versionen ab 6.32	-	-	-	6.51.0028

BESCHREIBUNG:

Eine kürzlich identifizierte Schwachstelle betrifft die Firmware von Bosch IP-Kameras ab Version 6.32. Wir bewerten diese Schwachstelle als kritisch, da sie potentiell einen unberechtigten Zugriff über die Netzwerkschnittstelle ermöglicht. Für IP-Kameras, die direkt aus dem öffentlichen Internet erreicht werden können, besteht ein erhöhtes Risiko.

Die Schwachstelle wurde von einem externen IT-Sicherheits-Forscher (VDOO) entdeckt und vertraulich an Bosch gemeldet. Am 12. Dezember 2018 wird Bosch ein Security Advisory veröffentlichen, in dem die wesentlichen Details der Schwachstelle bekannt gegeben werden. Danach ist auch mit einer Veröffentlichung weiterer Details durch VDOO zu rechnen.

Um die Schwachstelle zu schließen sind im Rahmen der nächsten Wartung Sicherheitsupdates auf allen betroffenen IP-Kameras zu installieren.

Es existiert zu diesem Thema noch eine weitere TI mit der Nummer 2207/2018. Diese wird als Änderungsklasse 1 veröffentlicht und betrifft einen kleineren Kundenkreis mit erhöhter Kritikalität zur sofortigen Durchführung.

Die Firmware-Updates finden Sie im Downloadstore: https://downloadstore.boschsecurity.com/index.php?type=FW

BEGRÜNDUNG:

Die Schwachstelle kann dazu ausgenutzt werden über das Netzwerk fremden Programmcode auf der IP-Kamera auszuführen. Darüber kann ein potentieller Angreifer Zugriffsbeschränkungen (Benutzername/Passwort) umgehen sowie kritische Funktionen (z.B. Sensorik/Aufzeichnung) auf der IP-Kamera ein- oder ausschalten. Ein Zugriff auf private Schlüssel im Trusted Computing Module (TPM) ist nicht möglich.

ABHILFE/ MAßNAHME:

Behoben wird die Schwachstelle mit einem Update auf die Firmware-Version 6.44.0027 oder höher (Release 6.4x) sowie 6.51.0028 oder höher (Release 6.5x). Bei einem Einsatz der IP-Kameras an einem Bosch Video Managementsystem (BVMS) gelten die folgenden empfohlenen Versionen der BU:

BVMS	CPP 7.3	CPP 7	CPP 6	CPP 4
7.0	6.44.0027	6.44.0027	6.44.0027	6.44.0027
7.5				
8.0				
9.0	6.51.0028	6.51.0028	6.51.0028	6.51.0028

Bei den BVMS Versionen 6.0 und 6.5 ist es aufgrund des Produktlebenszyklus möglich, dass eine betroffene Firmware im Einsatz sein könnte. Dabei besteht das Problem, dass die BVMS Versionen 6.0 und 6.5 in Kombination mit den gepatchten Firmware-Versionen NICHT freigegeben sind. In diesen Fällen ist ein Upgrade des BVMS Systems auf eine aktuelle Version erforderlich, da ansonsten kein Support mehr durch die BU geleistet wird. Bitte stornieren Sie in diesem Fall das Ticket und setzen Sie den Stornogrund auf „ST09 – Unterstützung erforderlich“. Der Vorgang wird dann zentral geprüft und weiterbearbeitet.

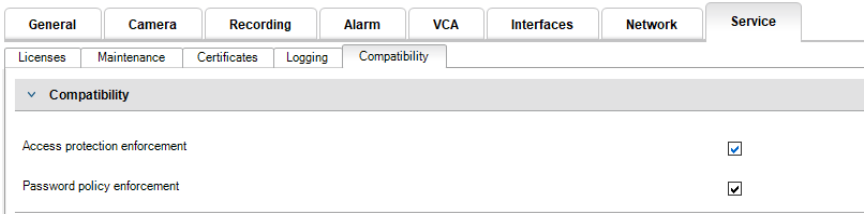
Bei älteren BVMS Versionen als 6.0 sollte eine Firmware-Version 6.32 oder höher nicht im Einsatz sein. Sollten Sie doch auf eine entsprechende Situation treffen, so verfahren Sie bitte wie bei der Version 6.0 beschrieben. Ein Downgrade der Firmware ist nicht zulässig.

HINWEISE:
Falls Ihrer Einschätzung nach ein Kunde bei der Ersteinschätzung einer zu niedrigen Kritikalität zugeordnet wurde, melden Sie diesen bitte kurzfristig an die ZSL (Reporting.ZSL@de.bosch.com). Wir prüfen dann die Einschätzung und stufen den Kunden bei Notwendigkeit neu ein.

Bitte beachten Sie neben der TI beim Update auch die allgemeinen Hinweise aus dem Release-Letter der jeweiligen Version.

Das Team der Videoleitstelle (CBS) hat die Kompatibilität der aktuellen Firmware-Versionen bestätigt.

Mit der Firmware-Version 6.40+ wurden zusätzliche Sicherheitsfunktionen (Zugriffsbeschränkungen, erforderliche Passwortkomplexität) eingeführt, die nach einem Update von einer Version < 6.40 automatisch aktiviert werden. Wir empfehlen diese Funktionen zu verwenden, da sie die Sicherheit der IP-Kameras zusätzlich erhöhen. Im Falle von Kompatibilitätsproblemen können die Funktionen aber über den ConfigManager im Reiter Service/Compatibility deaktiviert werden.



Die Auftragseröffnung mit Angabe der Tätigkeit erfolgt zentral über die Zentrale Service-Leitstelle (ZSL) in Magdeburg. Hierzu liegt der ZSL eine entsprechende Kundenliste mit allen betroffenen Installationen vor.

Wichtig: Eine ständig aktualisierte Liste mit Frequently Asked Questions (FAQ) sowie weiterführende Links zu dieser Schwachstelle finden Sie im WiKi des BT-IE Security Operations Center (SOC): https://inside-docupedia.bosch.com/confluence/display/IESOC/.

GESCHÄTZTE PLANZEIT:
35 Minuten zzgl. 3 Minuten je Komponente

ANLAGE:
► keine

Mit freundlichen Grüßen
Bosch Sicherheitssysteme GmbH

BT-IE/PRM3 Reutter

BT-IE/PRM1 Bernd Konopka

ANHANG A: LISTE DER BETROFFENEN HARDWARE:

Common Product Platform 7.3 (CPP7.3)	
Product family	**Fixed Firmware Versions**
AUTODOME IP 4000i	6.51.0028 6.50.0133
AUTODOME IP 5000i	
AUTODOME IP starlight 5000i (IR)	
AUTODOME IP starlight 7000i	
DINION IP bullet 4000i	
DINION IP bullet 5000i	
DINION IP bullet 6000i	
FLEXIDOME IP 4000i	
FLEXIDOME IP 5000i	
MIC IP starlight 7000i	
MIC IP fusion 9000i	

Common Product Platform 7 (CPP7)	
Product family	**Fixed Firmware Versions**
DINION IP starlight 6000	6.51.0028 6.50.0133 6.44.0027
DINION IP starlight 7000	
FLEXIDOME IP starlight 6000	
FLEXIDOME IP starlight 7000	
DINION IP thermal 8000	

Common Product Platform 6 (CPP6)	
Product family	**Fixed Firmware Versions**
DINION IP starlight 8000 12MP	6.51.0028 6.50.0133 6.44.0027
DINION IP ultra 8000 12MP	
DINION IP ultra 8000 12MP with C/CS mount telephoto lens	
FLEXIDOME IP panoramic 7000 12MP 180	
FLEXIDOME IP panoramic 7000 12MP 360	
FLEXIDOME IP panoramic 7000 12MP 180 IVA	
FLEXIDOME IP panoramic 7000 12MP 360 IVA	
AVIOTEC IP starlight 8000	
FLEXIDOME IP panoramic 6000 12MP 180	
FLEXIDOME IP panoramic 6000 12MP 360	
FLEXIDOME IP panoramic 6000 12MP 180 IVA	
FLEXIDOME IP panoramic 6000 12MP 360 IVA	

Common Product Platform 4 (CPP4)	
Product family	**Fixed Firmware Versions**
AUTODOME IP 4000 HD	6.51.0028 6.50.0133 6.44.0027
AUTODOME IP 5000 HD	
AUTODOME IP 5000 IR	
AUTODOME IP 7000 series	
DINION HD 1080p	
DINION HD 1080p HDR	
DINION HD 720p	
DINION imager 9000 HD	
DINION IP bullet 4000	
DINION IP bullet 5000	

Common Product Platform 4 (CPP4)	
Product family	**Fixed Firmware Versions**
DINION IP 4000 HD	
DINION IP 5000 HD	
DINION IP 5000 MP	
DINION IP starlight 7000 HD	
EXTEGRA IP dynamic 9000	
EXTEGRA IP starlight 9000	
FLEXIDOME corner 9000 MP	
FLEXIDOME HD 1080p	
FLEXIDOME HD 1080p HDR	
FLEXIDOME HD 720p	
Vandal-proof FLEXIDOME HD 1080p	
Vandal-proof FLEXIDOME HD 1080p HDR	
Vandal-proof FLEXIDOME HD 720p	
FLEXIDOME IP panoramic 5000	
FLEXIDOME IP indoor 5000 HD	
FLEXIDOME IP indoor 5000 MP	6.51.0028
FLEXIDOME IP indoor 4000 HD	6.50.0133
FLEXIDOME IP indoor 4000 IR	6.44.0027
FLEXIDOME IP outdoor 4000 HD	
FLEXIDOME IP outdoor 4000 IR	
FLEXIDOME IP micro 5000 HD	
FLEXIDOME IP micro 5000 MP	
FLEXIDOME IP outdoor 5000 HD	
FLEXIDOME IP outdoor 5000 MP	
FLEXIDOME IP micro 2000 HD	
FLEXIDOME IP micro 2000 IP	
IP bullet 4000 HD	
IP bullet 5000 HD	
IP micro 2000	
IP micro 2000 HD	
MIC IP dynamic 7000	
MIC IP starlight 7000	
TINYON IP 2000 family	