

Sicherheitsupdate – Abschaltung der Master-Passwort-Reset Seite durch FW

Register: Videosysteme/IP Kameras



BOSCH
Technik fürs Leben

Technische Information 2085/2017

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.
- III > Änderungen im Fehlerfall und bei Neuinstallationen einbringen
- Keine** > Allgemeine Information

Anzahl der betroffenen Systeme/Anlagen/Melder:	
-------------------------------------------------------	--

Hardware

Bezeichnung:	CTN	SAP-Nr.	Fertigungszeitraum
<ul style="list-style-type: none"> - CPP3 cameras and encoders - VIP X1600 XFM4 - VJT X20/X40 XF-E - VJT XTC XF - VIDEOJET Decoder 3000 			

Software

Bezeichnung:	CTN	SAP-Nr.	Version alt	Version neu
<ul style="list-style-type: none"> - Firmware 5.53.0001 - Firmware 5.74.0001 - Firmware 5.97.0002 				

- Beschreibung:** Kürzlich durchgeführte Penetrationstests haben eine Sicherheitslücke aufgezeigt, welche den Mechanismus zur Passwort-Rücksetzung aller Geräte kleiner dem Firmwarestand 6.20 betreffen.
- Um das Sicherheitsproblem zu beheben, wurde ein Maintenance-Update in der FW 5.53, 5.74 und 5.97 durchgeführt. Im Update wurde die Seite für die Passwortrücksetzung vollständig entfernt.
- Nun gilt es bei der Rücksetzung des Passworts folgende wichtige Hinweise zu beachten.
- Hintergrund** Moderne Plattformen, darunter CPP4 und neuer, werden weiterhin mit Firmware-Feature-Releases gepflegt und erhalten somit auch regelmäßig Sicherheitsverbesserungen. Für diese Plattformen wurde der Passwort-Freischaltungsmechanismus bereits 2015 mit der FW 6.20 zu einem sichereren, zertifikatsbasierten Algorithmus geändert.
- Wenn das Gerät direkt mit dem Internet oder einem nicht-exklusiven Firmen- oder Büronetzwerk verbunden ist, wird dringend empfohlen, auf diese Version upzugraden, um die Sicherheitsanfälligkeit zu beseitigen.
- Die Aktualisierung auf FW 6.20 oder höher beseitigt die Anfälligkeit des alten Mechanismus, der Anfang 2000 eingeführt wurde und somit auch die Sicherheitslücke.
- Die Kennwort-Freischaltungen für CPP3 und CPP-ENC Geräte, welche noch nicht mit der o.g. FW upgedatet wurden, kann ebenfalls nicht mehr wie gewohnt telefonisch über den ST-IE/PRM-Support erfolgen. Hier wurden die Rechte auf den Level 3 Support der BU beschränkt.
- Abhilfe:** **Passwortrücksetzung bei ...**
- A) Geräte, welche noch nicht mit der o.g. FW upgedatet wurden:
- Ticket im BoCams öffnen; ST-IE/PRM eröffnet darauf ein Ticket bei ST/ASA im Level 3 Support
 - ST/ASA setzt nach Absprache zusammen mit Techniker das Passwort zurück
- B) Geräte, welche bereits mit der o.g. FW upgedatet wurden:
- hier besteht keine Möglichkeit, über den Support das PW zurückzusetzen
 - Da kaum noch ein Gerät über den „Factory Reset Knopf“ verfügt, muss das Gerät an ST/ASA eingeschickt werden.
- C) Geräte, welche mit der FW 6.20 und höher laufen:
- Die Kennwort-Freischaltungen ab FW 6.20 können weiterhin vom ST-IE/PRM-Support durchgeführt werden.

Hinweise: Falls ein Passwort vergessen wurde, besteht bei den Geräten, wo der Rücksetzmechanismus entfernt wurde, keine Zugriffsmöglichkeit mehr.

Bosch Connect: https://connect.bosch.com/blogs/0aae1084-9ba7-4231-b306-46c90a86674f/entry/Security_Fix_Maintenance_FW_releases?lang=de_de

Weiterhin gültige SW: Siehe FW Maintenance-Release

Anlage: [Bosch_Releaseletter_CPP-ENC_H.264_FW_5.53.0001.pdf](#)
[Bosch_Releaseletter_CPP3_H.264_FW_5.74.0001.pdf](#)
[Bosch_Releaseletter_CPP-ENC_H.264_FW_5.97.0002.pdf](#)

Mit freundlichen Grüßen

Bosch Sicherheitssysteme GmbH

ST-IE/PRM3 Reutter

ST-IE/PRM1 Konopka