

BALLUFF



IO-Link Topologie meets CRA

Firmware, Usermanagement und Dokumentation im Griff

Jan-Erik Jung



Produktmanager Systeme



Balluff GmbH



+49 173 150 0378



jan-erik.jung@balluff.de



FIRMWARE-ÜBERSICHT

● Device Group A	v1.2.3 >
● Device Group B	v2.4.1 >
● Device Group C	v1.0.8 >
● Device Group D	v2.3.0 >

ZUGRIFF & BENUTZER

👤 Admin	Vollzugriff
👤 Service	Wartung
👤 Operator	Read-Only



LINE 1 - IO-LINK MASTER

FW: 2.4.1
Status: OK



ROBOT CELL 04

FW: 1.0.8
Status: Vulnerability



3

kritisch

7

mittel

BALLUFF

ZENTRALE AKTIONEN

- 🔄 Firmware-Update planen
- 🛡️ Security-Patch verteilen
- ⚙️ Konfiguration prüfen



PACKAGING LINE

FW: 2.3.0
Status: OK



CONVEYOR 12

FW: 1.0.6
Status: Vulnerability



SENSOR STATION 7

FW: 2.4.1
Status: OK



ZENTRALES MANAGEMENT



Inventar



Firmware



Sicherheit



Benutzer



Berichte

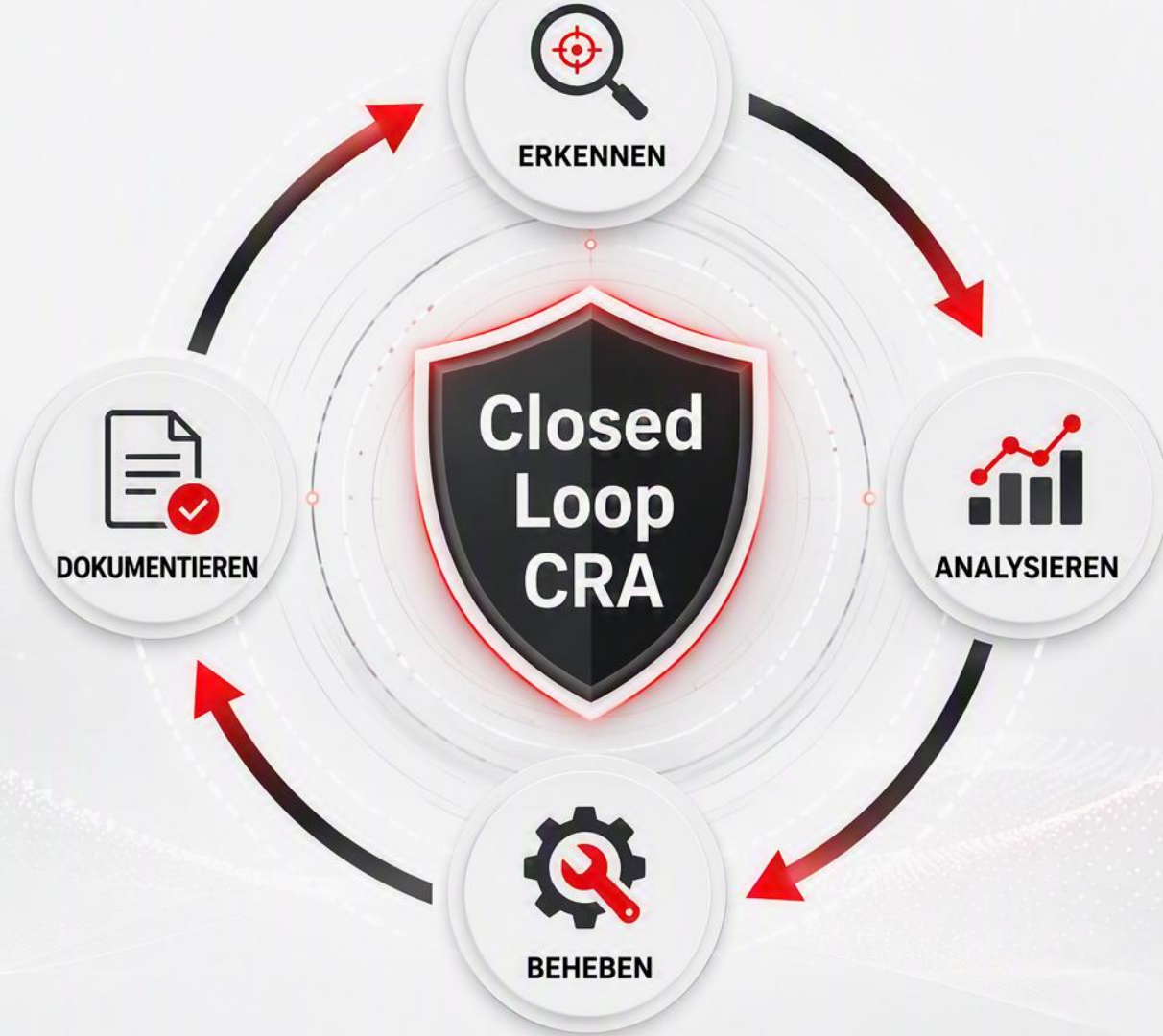


DRIVE UNIT 3

FW: 1.1.2

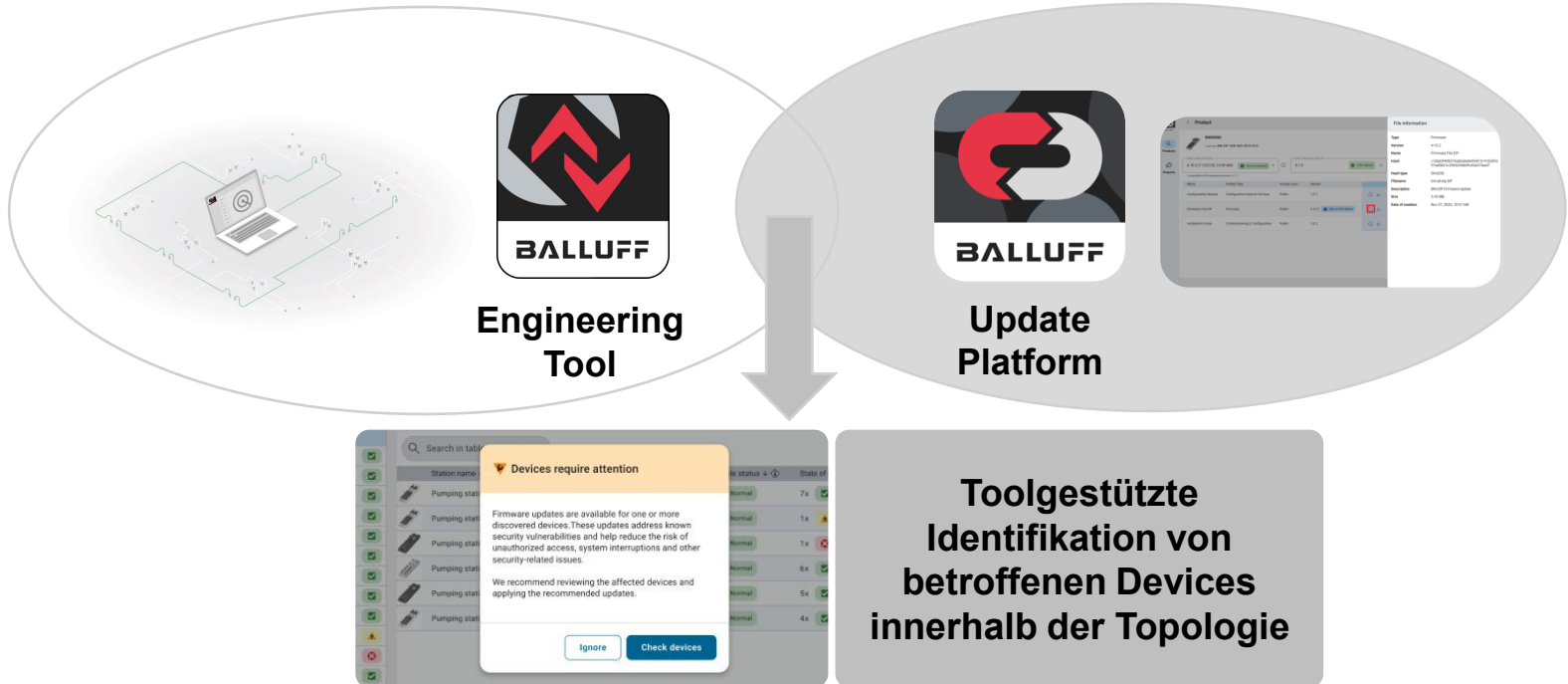
Update verfügbar







STEP 1: Erkennen





STEP 2: Analysieren



Update Platform



Products

Advisories

< Advisories

Balluff GmbH: Multiple Vulnerabilities Affecting BNI EGW-720-007-K095 and BAV MA-NC-00025-01

VDE ID

[VDE-2026-049](#)

CSAF Document

[Download](#)

Last update

6/30/26, 12:00 PM

Published at

6/30/26, 12:00 PM

Affected Products

[BAV MA-NC-00025-01](#) (BAV MA-NC-00025-01 Firmware <2.4.1)

[BNI EGW-720-007-K095](#) (BNI EGW-720-007-K095 Firmware <2.4.1)

Summary

Security advisory for Balluff BNI EGW-720-007-K095 and BAV MA-NC-00025-01 firmware versions prior to 2.4.1. This advisory covers multiple vulnerabilities affecting software components used by the device firmware.

Impact

Multiple vulnerabilities in software components used by the affected product could allow remote or local attackers, depending on the specific issue, to cause denial of service, disclose sensitive information, escalate privileges, or affect the integrity of the device and its services. The concrete impact depends on the affected component and the deployment context.

Remediation

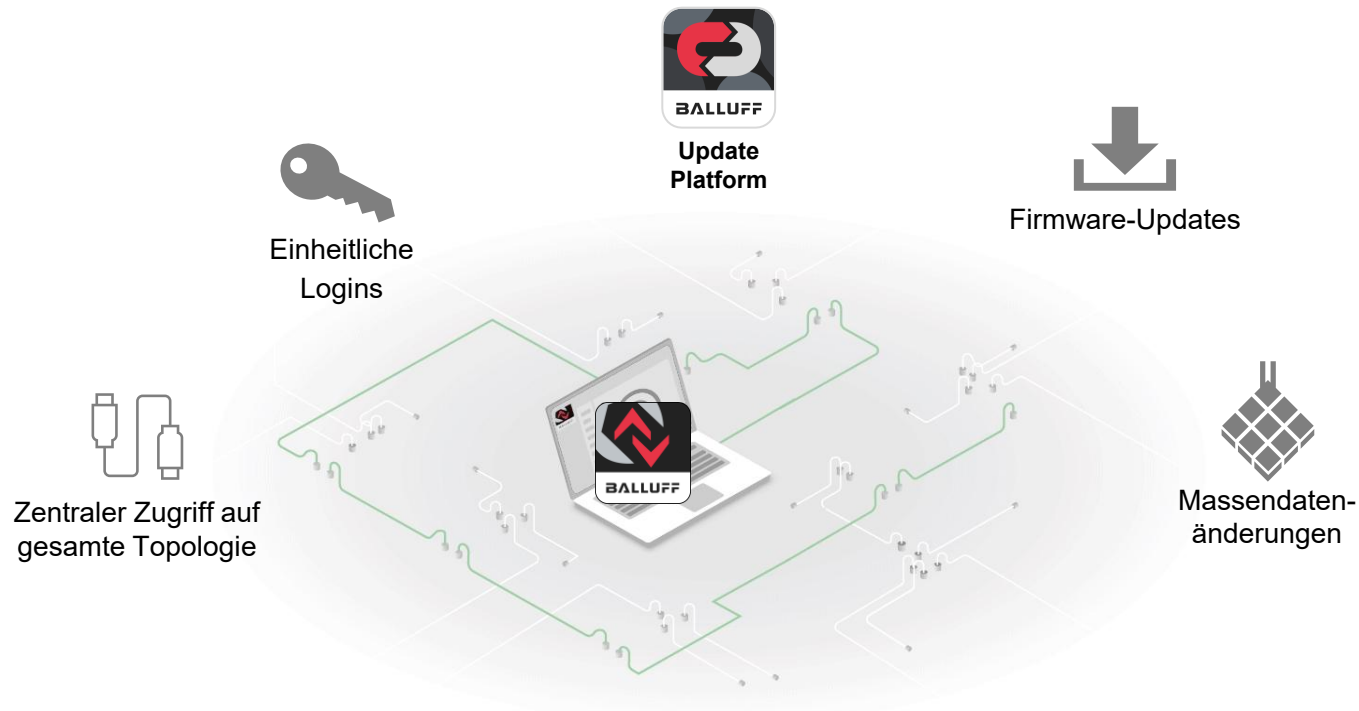
Update the firmware of BNI EGW-720-007-K095 and BAV MA-NC-00025-01 to version 2.4.1 or later. The fixed firmware contains updates for the vulnerabilities covered by this advisory.

Detaillierte Beschreibung des CVE inkl. Handlungsempfehlung

* CVE: Common Vulnerabilities and Exposures



STEP 3: Beheben



Minimaler Aufwand mit Hilfe des Balluff Engineering Tools

STEP 4: Dokumentieren



**Engineering
Tool**

Balluff Engineering Tool

Zur Projektübersicht

Search

Unbenannte Topologie

- BNIO0K7
- BIS M-4A9-082-401-07-...
- BCM0001
- BNIO087

Testaufbau

Standort Neuhausen | Beschreibung

Übersicht Zustände Authentifizierung Protokolle Firmware-Aktualisierung **Geräteliste**

In Tabelle suchen

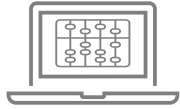
IPv4 Adresse	Port	Verbindungsstatus	Produkt-ID	Geräte-ID	Seriennummer	Hersteller	MAC Adresse	ID-Link Revision	Firmwareversion	Hardwareversion
169.254.0.9		Verbunden	BNIO0K7	10507569	HU00943352100039	Balluff	00-19-31-55-DD-33	nicht anwendbar	1.1.0	1.0.0
nicht anwendbar	0	Verbunden	BIS M-4A9-082-401-07-PU1-0,3 (CCM)	393783	nicht anwendbar	Balluff	nicht anwendbar	V1.1	1.3.0	1.0
nicht anwendbar	1	Verbunden	BCM0001	917761	nicht anwendbar	Balluff	nicht anwendbar	V1.1	v3.04.013	v2.1
nicht anwendbar	3	Verbunden	BNIO087	330246	nicht anwendbar	BALLUFF	nicht anwendbar	V1.1	4.1 2019/04/10 14:51:36 R 4272	2

Schließen Exportieren

Dokumentation und Back-up des neuen IST-Zustands



**Ein Tool für alle
Hersteller**



**Parametrieren
ohne Hardware**



**Indiv. Geräte-
beschreibungs-
dateien erstellen**



**Engineering
Tool**



**Auslieferungszustand
wiederherstellen**



**Prozessdaten-
visualisierung**



**Konfiguratoren
unterstützen beim
Parametrieren**

Kostenfreier Download – probieren Sie es aus!

Contact us!



Jan-Erik Jung



Stand 703



Balluff Engineering Tool

BALLUFF

 *innovating automation*

www.balluff.com