Bender GmbH & Co. KG

Bender Security Advisory BENDER-2019-001

Title
COMTRAXX Vulnerability - Inadequate Credentials check

Rating
medium

Affected Products

Device	Order number	Affected versions
COM465IP	B95061065, B95061066	<4.2.1
COM465DP	B95061060, B95061061	<4.2.1
COM465ID	B95061070	<4.2.1
CP700	B95061030	<4.2.1
CP907	B95061080	<4.2.1
CP915	B95061081, B95061085, B95061092	<4.2.1

Summary
Bender is publishing this advisory to inform customers about a security vulnerability in all devices running the COMTRAXX software.

The user authorization is validated for most, but not all routes in the system. A user with knowledge about the routes can read and write configuration data without prior authorization.

Impact
The vulnerability allows a malicious entity to bypass credential check.

Mitigation
- restrict network access to the above-mentioned devices
- install latest software update

Security Updates

Please install V4.2.1. (https://www.bender.de/service-support/downloadbereich)

Vulnerability Characterization and CVSSv3 Rating

CWE-287: Improper Authentication link
CVSS: 8.2 **High** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N link

Acknowledgements
Bender would like to thank Maxim Rupp for reporting the issue. The issue was coordinated by CERT@VDE.

CVE-ID CVE-2019-19885