PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

07 June 2021
300506988

# Security Advisory for Automation Worx Software Suite

## Advisory Title

Phoenix Contact Automationworx BCP File Parsing Memory Corruption Remote Code Execution Vulnerability

## Advisory ID

VDE-2021-020
CVE-2021-33542

ZDI-CAN-13134

## Vulnerability Description

Manipulated PC Worx or Config+ projects could lead to a remote code execution when unallocated memory is freed because of incompletely initialized data (CWE-824).
The attacker needs to get access to an original bus configuration file (*.bcp) to be able to manipulate data inside. After manipulation the attacker needs to exchange the original file by the manipulated one on the application programming workstation.

## Affected products

Following components of Automationworx Software Suite version 1.87 and earlier are affected:

- PC Worx
- PC Worx Express
- Config+

## Impact

Availability, integrity, or confidentiality of an application programming workstation might be compromised by attacks using these vulnerabilities.
Automated systems in operation which were programmed with one of the above-mentioned products are **not** affected.

## Classification of Vulnerability

Base Score: 7.8
Vector: CVSS: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

## Temporary Fix / Mitigation

We strongly recommend customers to exchange project files only using secure file exchange services. Project files should not be exchanged via unencrypted email.

## Remediation

With the next version of Automationworx Software Suite the affected data will be initialized completely and thereby freeing of unallocated memory will be prevented.

## Acknowledgement

The vulnerability was discovered by Francis Provencher {PRL} and reported by Zero Day Initiative (ZDI).

PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.