

2020-02-24  
300440147/pbsa56

## Security Advisory for Automation Worx Software Suite – Update 2020-02-24

### Advisory Title

Phoenix Contact Automationworx BCP File Parsing:  
Uninitialized Pointer Remote Code Execution Vulnerability, Use-After-Free Remote Code  
Execution Vulnerability and Out-Of-Bounds Read Information Disclosure Vulnerability

### Advisory ID

VDE-2019-014

CVE-2019-12869 (ZDI-CAN-7781)  
CVE-2019-12870 (ZDI-CAN-7784)  
CVE-2019-12871 (ZDI-CAN-7780, ZDI-CAN-7785, ZDI-CAN-7786)

### Vulnerability Description

A manipulated PC Worx or Config+ project file could lead to a remote code execution.  
The attacker needs to get access to an original PC Worx or Config+ project file to be able to  
manipulate it. 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 1.86 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**

ZDI-CAN-7780, -7784, -7785, -7786:

Base Score: 7.8

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

ZDI-CAN-7781:

Base Score: 3.3

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

### **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 following measures will be implemented:

- The zlib component will be updated to the latest version (1.2.11.0). By utilizing the latest version of zlib a manipulated BCP file is detected as corrupt. The unpacking operation is aborted and therefor the remote code execution is precluded.
- The validation of input data will be improved.
- Objects in the affected software components will be completely initialized.
- Further 3<sup>rd</sup> party components will be checked for known vulnerabilities and will be exchanged or updated if required.
- General preventive security measures will be implemented such as address space layout randomization.

**Update 2020-02-24:** Above-mentioned improvements have been implemented in Automationworx Software Suite 1.87 which is available for [download](#) now.

### **Acknowledgement**

The vulnerabilities were discovered by 9sg Security Team.  
Reported through Zerodayinitiative.  
Coordinated by NCCIC and CERT@VDE.