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

2020-02-24
300440147/pbsa56

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

Advisory Title

Phoenix Contact Automationworx Suite:
*.bcp-file Memory Corruption Remote Code Execution Vulnerability and *.mwt-file Out-Of-Bounds Read Remote Code Execution Vulnerability

Advisory ID

VDE-2019-016
CVE-2019-16675

ZDI-CAN-7782
ZDI-CAN-8097

Vulnerability Description

Manipulated PC Worx or Config+ projects could lead to a remote code execution due to insufficient input data validation.

The attacker needs to get access to an original PC Worx or Config+ project to be able to manipulate data inside the project folder. After manipulation the attacker needs to exchange the original files by the manipulated ones 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

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 a sharpened validation of arrays regarding dimension and number of elements during input data conversion will be implemented.
To improve the robustness against manipulated project files the input data validation will be extended.
Further preventive security measures will be activated in the compiler settings.

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.