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

26 March 2021
300478795

Security Advisory for Automation Worx Software Suite

Advisory Title

Phoenix Contact Automation Worx Software Suite vulnerabilities:
PLCopen XML file parsing stack-based buffer overflow and *.mwe file parsing out-of-bounds read remote code execution

Advisory ID

VDE-2020-023
CVE-2020-12497 (ZDI-CAN-10147, ZDI-CAN-12244)
CVE-2020-12498 (ZDI-CAN-10586)

Vulnerability Description

Manipulated PC Worx 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 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 Automation Worx Software Suite version 1.87 and earlier are affected:

- PC Worx
- PC Worx Express

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.
In addition, we recommend exchanging or storing project files together with a checksum to ensure their integrity.

Remediation

With the next version of Automation Worx Software Suite a sharpened input data validation with respect to buffer size and description of size and number of objects referenced in a file will be implemented.

Update A 2021-03-26: The updated version of the Automation Worx Software Suite (V1.88) that fixes the vulnerabilities described in this advisory is available for download now.

Acknowledgement

The vulnerability ZDI-CAN-10147, ZDI-CAN-12244 was discovered by Natnael Samson working with Trend Micro Zero Day Initiative.

The vulnerability ZDI-CAN-10586 was discovered by mdm working with Trend Micro Zero Day Initiative