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

03 November 2021
300524563

Security Advisory for Automation Worx Software Suite

Advisory Title

Phoenix Contact Automation Worx Software Suite vulnerabilities:
PC Worx is vulnerable to a “zip slip” style vulnerability when loading a project file.

Advisory ID

VDE-2021-052
CVE-2021-34597

Vulnerability Description

A maliciously crafted project archive could allow an attacker to unpack arbitrary files outside of the selected project directory (CWE-20).

The attacker needs to get access to an original PC Worx project archive to be able to manipulate data inside the archive. After manipulation the attacker needs to exchange the original file by the manipulated one on the application programming workstation.

Affected products

Following components of Automation Worx Software Suite version 1.88 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 additional plausibility checks for archive content will be implemented.

Acknowledgement

The vulnerability was discovered by Jake Baines of Dragos Inc.
We kindly appreciate the coordinated disclosure of these vulnerabilities by the finder.

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