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

08 November 2022
2022/00004

Security Advisory for Automation Worx Software Suite

Publication Date: 2022-11-08
Last Update: 2022-11-15
Current Version: V1.1

Advisory Title

Phoenix Contact Automationworx BCP File Parsing Vulnerabilities

Advisory ID

CVE-2022-3461
CVE-2022-3737

VDE-2022-048

Vulnerability Description

Manipulated PC Worx or Config+ files could lead to a heap buffer overflow, release of unallocated memory or a read access violation due to insufficient validation of input data. 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 1.89 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.

Classification of Vulnerability

Heap Buffer Overflow
CVE: CVE-2022-3461
Base Score: 7.8
Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CWE: CWE-119

Read Access Violation
CVE: CVE-2022-3737
Base Score: 7.8
Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CWE: CWE-125

CVE score and vector may have changed since publication of this advisory. You can find the current rating of a CVE at the respective link to the NVD website provided above.

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 an already implemented remediation measure needs to be corrected to prevent the release of unallocated memory.
To prevent the read access violation the validation of the input data will be improved.
We strongly recommend customers to upgrade to Automation Worx Software Suite > 1.89.

Acknowledgement

This vulnerability was discovered and reported by Michael Heinzl.
We kindly appreciate the coordinated disclosure of this vulnerability by the finder.

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

History

V1.0 (2022-11-08): Initial publication
V1.1 (2022-11-15): Removed sentence "Automated systems in operation which were programmed with one of the abovementioned products are not affected." from Impact section.