Phoenix Contact Inc.
P.O. BOX 4100
Harrisburg, PA 17111-0100
Phone: 717-944-1300
Fax: 717-944-1625

Product Change Notification

PCN-AS-6760-2021

Business Unit	Product Line Code	Type of Change	Action	Date of Issue
AS - Automation Systems	DRA	Product Change Notification	Notify Distributors and Field	3/30/2021

The following Phoenix Contact products have been modified. Existing specifications will be met or exceeded. Please review and acknowledge this document and inform your personnel as needed.

Product Change Notification

Description for Product Change Notification

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)
CVE-2020-12498 (ZDI-CAN-10586)

Vulnerability Description
Manipulated PC Worx projects could lead to a remote code execution due to insufficient inputdata 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 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.

Stock Status

Can existing stock still be used?

Is mixture of stock acceptable?

Product Change Notification

Transaction Dates	
Date modification goes into effect from Germany:	3/30/2021
Expected first shipment (from Phoenix Contact) of the modified products(s):	3/30/2021

Should you have any issues with the timeline or content of this product change, please contact Phoenix Contact using the information below. Customers should acknowledge receipt of the PCN within 30 days of delivery of the PCN; provided, however, that the failure to acknowledge receipt does not affect the product change or the effective date thereof.

Contact Info:
Yuri Chamarelli
ychamarelli@phoenixcontact.com

Thank you,

Zachary Stank

Product Marketing Manager

Product Change Notification

Part #	Type Description
2701034	ILC 131 ETH/XC
2700976	ILC 191 ETH 2TX
2700973	ILC 131 ETH
2700974	ILC 151 ETH
2700975	ILC 171 ETH 2TX
2701141	ILC 151 ETH/XC
2985314	ILC 390 PN 2TX-IB
2876928	ILC 350 PN
2985576	ILC 370 PN 2TX-IB/M
2404577	RFC 480S PN 4TX
2916794	RFC 470S PN 3TX
2700784	RFC 460R PN 3TX
2700988	AXC 1050
2700989	AXC 3050
2985275	PC WORX BASIC LIC
2985385	PC WORX PRO LIC
2988670	PC WORX EXPRESS