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

25 March 2020
300469050/pbsa56

Security Advisory for PC WORX SRT - 2701680

Advisory Title

Unprivileged user can override the main service of ‘PC WORX SRT’ under the Phoenix Contact installation path, and therefore, escalate to run code as SYSTEM user and gain local privilege escalation.

Advisory ID

VDE-2020-012
CVE-2020-10939

Vulnerability Description

Phoenix Contact application ‘PC WORX SRT’ is installed as service. The installation path of the application is configured to have insecure permissions which allows any unprivileged user to write arbitrary files to the installation directory where all the configuration files and binaries of the service are located.

Affected products

Product	Article number	Affected versions
PC WORX SRT	2701680	<=1.14

Impact

A malicious user can leverage this knowledge and override the main ‘PC WORX SRT’ service with a rogue binary which will result with running malicious code as SYSTEM user.

Classification of Vulnerability

Base Score: 7.8
Vector: CVSS: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Personally liable partner:	Group Executive Board:	Deutsche Bank AG	Commerzbank AG
Phoenix Contact Verwaltungs GmbH	Frank Stührenberg (CEO)	(BLZ 360 700 50) 226 2665 00	(BLZ 476 400 51) 226 0396 00
Amtsgericht Lemgo HRB 5273	Roland Bent	BIC: DEUTDEDEXXX	BIC: COBADEFFXXX
Kom. Ges. Amtsgericht Lemgo HRA 3746	Prof. Dr. Gunther Olesch	IBAN:	IBAN:
	Axel Wachholz	DE93 3607 0050 0226 2665 00	DE31 4764 0051 0226 0396 00

...

Temporary Fix / Mitigation

Customers using PC WORX SRT are strongly recommended to use the software only on single user systems where restricting the access rights of the PC WORX SRT is not necessary.

Phoenix Contact strongly recommends protection measures against unauthorized access for network-compatible devices, solutions and PC-based software. For detailed information please refer to our application note:

Measures to protect network-compatible devices with communication interfaces, solutions and PC-based software against unauthorized access

Acknowledgement

This vulnerability was discovered and reported to Phoenix Contact by Sharon Brizinov of Claroty.