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

16 July 2020
300481631/pbsa56

Security Advisory for PLCNEXT ENGINEER

Advisory Title

Improper path sanitation on import of project files in PLCnext Engineer.

Advisory ID

CVE-2020-12499
VDE-2020-025

Vulnerability Description

The build settings of a PLCnext Engineer project (.pcwex) can be manipulated in a way that can result in the execution of remote code.
The attacker needs to get access to a PLCnext Engineer project to be able to manipulate files inside. Additionally, the files of the remote code need to be transferred to a location which can be accessed by the PC that runs PLCnext Engineer. When PLCnext Engineer runs a build process of the manipulated project the remote code can be executed.

Affected products

Article no	Article	Affected versions	Download
1046008	PLCnext Engineer	2020.3.1 and earlier	download

Impact

Availability, integrity, or confidentiality of an engineering workstation might be compromised by attacks using these vulnerabilities.

Personally liable partner:
Phoenix Contact Verwaltungs GmbH
Amtsgericht Lemgo HRB 5273
Kom. Ges. Amtsgericht Lemgo HRA 3746

Group Executive Board:
Frank Stührenberg (CEO)
Roland Bent
Prof. Dr. Gunther Olesch
Axel Wachholz

Deutsche Bank AG
(BLZ 360 700 50) 226 2665 00
BIC: DEUTDEDEXXX
IBAN:
DE93 3607 0050 0226 2665 00

Commerzbank AG
(BLZ 476 400 51) 226 0396 00
BIC: COBADEFFXXX
IBAN:
DE31 4764 0051 0226 0396 00

...

Classification of Vulnerability

Base Score: 8.2
Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/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. Users should avoid importing project files from unknown source and exchange or store project files together with a checksum to ensure their integrity.

Remediation

Phoenix Contact strongly recommends updating to the latest version PLCnext Enineer 2020.6 or higher, which fixes this vulnerability.

Acknowledgement

This vulnerability was discovered and reported by Amir Preminger of Claroty.

We kindly appreciate the coordinated disclosure of this vulnerability by the finder.