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
300465884/pbsa56

Security Advisory for Portico Remote desktop control software

Advisory Title

Privilege escalation in Portico Remote desktop control software.

Advisory ID

VDE-2020-013
CVE-2020-10940

Vulnerability Description

If the software runs as a service, a user with limited access can gain administrator privileges by starting a shell with administrator rights from the Import / Export configuration dialog.

Affected products

Article number	Article name	Affected versions
2701453	PORTICO SERVER 1 CLIENT	<= 3.0.7
2701455	PORTICO SERVER 4 CLIENT	<= 3.0.7
2701456	PORTICO SERVER 16 CLIENT	<= 3.0.7

Impact

A malicious user could use this vulnerability to gain administrator privileges on the Computer running the Portico software.

...

Classification of Vulnerability

Base Score: 7.8
Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Remediation

Phoenix Contact strongly recommends users to upgrade to Portico V3.0.8 or higher which fixes this vulnerability. The current version of Portico is available on the Phoenix Contact website at following address: www.phoenixcontact.net/qr/2701453/softw

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

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