

[← VDE-2019-015 \(/en/advisories/VDE-2019-015/\)](/en/advisories/VDE-2019-015/) (../)[VDE-2022-026 → \(/en/advisories/VDE-2022-026/\)](/en/advisories/VDE-2022-026/)**2022-06-21 07:15 (CEST)****VDE-2022-025**

## PHOENIX CONTACT: Vulnerability in classic line industrial controllers

**Share:** Email | (mailto:?subject=CERT@VDE has released a new advisory&body=VDE-2022-025:

PHOENIX%20CONTACT%3A%20Vulnerability%20in%20classic%20line%20industrial%20controllers (URL:

http://localhost/en/advisories/VDE-2022-025//en/advisories/VDE-2022-025/)) Twitter

(https://twitter.com/intent/tweet?url=http://localhost/en/advisories/VDE-2022-025//en/advisories/VDE-2022-025/&text=CERT@VDE has released a new advisory: VDE-2022-

PHOENIX%20CONTACT%3A%20Vulnerability%20in%20classic%20line%20industrial%20controllers) 

**ID** VDE-2022-025

**Published** 2022-06-21 07:15 (CEST)

**Last update** 2022-06-21 07:15 (CEST)

**Vendor(s)** PHOENIX CONTACT GmbH & Co. KG

**Product(s)**




Article No°	Product Name	Affected Version(s)
	AXC 1050	all versions
2701295	AXC 1050 XC	all versions
2700989	AXC 3050	all versions
2730844	FC 350 PCI ETH	all versions
	ILC1x0	all versions
	ILC1x1	all versions
2700977	ILC 1x1 GSM/GPRS	all versions
	ILC 3xx	all versions
2700291	PC WORX RT BASIC	all versions

2701680	PC WORX SRT	all versions
2730190	RFC 430 ETH-IB	all versions
2730200	RFC 450 ETH-IB	all versions
2700784	RFC 460R PN 3TX	all versions
1096407	RFC 460R PN 3TX-S	all versions
2916600	RFC 470 PN 3TX	all versions
2916794	RFC 470S PN 3TX	all versions
2404577	RFC 480S PN 4TX	all versions

## Summary

The affected devices insufficiently verify uploaded data.

---

CVE ID	CVE-2022-31800 ( <a href="https://nvd.nist.gov/vuln/detail/CVE-2022-31800">https://nvd.nist.gov/vuln/detail/CVE-2022-31800</a> ) 
Last Update:	Nov. 17, 2022, 11:18 a.m.
Severity	<b>9.8</b> (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) ( <a href="https://nvd.nist.gov/vuln">https://nvd.nist.gov/vuln</a> )
Weakness	Insufficient Verification of Data (CWE-345) Authenticity ( <a href="https://cwe.mitre.org/data/definitions/345.html">https://cwe.mitre.org/data/definitions/345.html</a> ) 
Summary	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device.
Details	<a href="https://nvd.nist.gov/vuln/detail/CVE-2022-31800">nvd.nist.gov</a> ( <a href="https://nvd.nist.gov/vuln/detail/CVE-2022-31800">https://nvd.nist.gov/vuln/detail/CVE-2022-31800</a> ) 

---

## Impact


An attacker capable of either transmitting manipulated logic or manipulating legitimate logic can execute arbitrary malicious code on the device.

## Solution

## Mitigation

Phoenix Contact classic line controllers are designed and developed for the use in closed industrial networks. The controller doesn't feature logic integrity and authenticity checks by design. Phoenix Contact therefore strongly recommends using the devices exclusively in closed networks and protected by a suitable firewall.

Customers using Phoenix Contact classic line controllers are recommended to operate the devices in closed networks or protected with a suitable firewall as intended.

Generic information and recommendations for security measures to protect network-capable devices can be found in the application note ([https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913\\_en\\_03.pdf](https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf)) .

## Reported by

This vulnerability was reported by Forescout.

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.

---

## Member of



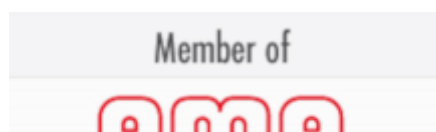
(<https://www.cert-verbund.de/>)



(<https://www.trusted-introducer.org/directory/teams/vde.html>)



(<https://www.allianz-fuer-cybersicherheit.de/>)



(<https://www.ama-sensorik.de/>)

---

[Contact \(/more/certvde/contact\)](/more/certvde/contact) | [Imprint \(https://www.vde.com/en/legal-notice\)](https://www.vde.com/en/legal-notice) | [Privacy Statement \(/more/certvde/privacy-statement\)](/more/certvde/privacy-statement) | [Data Protection Notice \(/more/certvde/data-protection-notice\)](/more/certvde/data-protection-notice)