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

14. August 2020
300488745 / pbsa56

Security Advisory for Emalytics, ILC 2050 BI and ILC 2050 BI-L

Advisory Title

TLS Timeout Vulnerability.

Advisory ID

CVE-2020-14483
VDE-2020-026

Vulnerability Description

A timeout during a TLS handshake can result in the connection failing to terminate. This can result in a Niagara thread hanging and requires a manual restart to correct.

Affected products

Article	Article number
ILC 2050 BI	2403160
ILC 2050 BI-L	2404671
Emalytics Automation Workbench N4	

Firmware versions related to Emalytics Automation up to and including version 1.3.0 (Niagara versions 4.6.96.28, 4.7.109.20, 4.7.110.32, 4.8.0.110).

Impact

Successful exploitation of this vulnerability could result in a denial-of-service condition.

Classification of Vulnerability

Base Score: 4.3
Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Mitigation

Phoenix Contact recommends customers with affected products take the following steps to protect themselves:

- Review and validate the list of users who are authorized and who can authenticate to Emalytics.
- Allow only trained and trusted persons to have physical access to the system, including devices that have connection to the system though the Ethernet port.

Phoenix Contact recommends operating network-capable devices in closed networks or protected with a suitable firewall. For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note:

Art.-Nr. 107913: AH EN INDUSTRIAL SECURITY “Measures to protect network-capable devices with Ethernet connection against unauthorized access”

Remedation

This vulnerability will be fixed in the regular firmware release (v.1.4.0) which is expected to be available October 2020.

Acknowledgement

Honeywell reported this vulnerability to CISA.