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

13 February 2020
300472504 / pbsa56

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

Advisory Title

Remote configuration using unauthenticated web server access.

Advisory ID

CVE-2020-8768
VDE-2020-001

Vulnerability Description

Phoenix Contact Emalytics Controllers ILC 2050 BI are developed and designed for the use in protected building automation networks. A link on the website of the devices allows unauthorized read and write access to the configuration of the devices. Application and application data are not affected.

Affected products

Article	Article number
ILC 2050 BI	2403160
ILC 2050 BI-L	2404671

Firmware versions related to Emalytics up to version 1.2.1.

Impact

If the above-mentioned controllers are used in an unprotected open network, an unauthorized attacker can change the device configuration and start or stop services.

Classification of Vulnerability

Base Score: 9.4
Vector: CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

...

Temporary Fix / Mitigation / Remedation

Phoenix Contact strongly recommends affected users to update to Engineering software Emalytics 1.2.3 or higher and recommission the controllers.

Please note: If this is not possible, please contact us via email at
development.sysmik@phoenixcontact.com
so that we can provide you with a fixed version.

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”

Acknowledgement

This vulnerability was discovered by Mr. Anil Parmar.