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

Phoenix Contact GmbH & Co. KG mitigation advice for ILC 150 Webvisit ETH authentication vulnerability

ICS-CERT Released: November 8, 2016, ICSA-16-313-01
CVE-2016-8366, CVE-2016-8371, CVE-2016-8380

Overview:
Phoenix Contact was made aware about a Webvisit authentication vulnerability in its ILC 150 ETH PLC’s. Phoenix Contact is recommending that customers take steps to mitigate this potential threat.
ILC 150 ETH is offering a Webserver based HMI system configured by the Engineering tool Webvisit. Phoenix Contact is preparing an Update that mitigates this vulnerability.

Affected Products:
All ILC 1xx PLC’s of Phoenix Contact

Vulnerability Details:
The identified vulnerability allows unauthenticated users to access HMI pages and to modify PLC variables.

1. Webvisit offers a password macro to protect HMI pages on the PLC against casual or coincidental opening of HMI pages by the user. The password macro can be configured in a way that the password is stored and transferred in clear text.

2. The Webserver is able to be accessed by HTTP gets and posts even if the former authentication mechanism is enabled.

3. The Webserver is providing data of global PLC variables which are not used in the HMI application via HTTP gets and posts

Mitigation:
Connecting devices to a network via Ethernet always entails the risk of unauthorized access to the network. Phoenix Contact recommends that users implement an adequate defense–in-depth networking architecture for control systems where these devices are operating.

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

Executive Vice Presidents:
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

...

1. It is highly recommended that the devices are not exposed to public networks without the use of virtual private networks (VPNs) for remote access, as well as the use of firewalls for network segmentation or controller isolation.

2. Available communication channels or ports not needed in the application should be turned off. Therefore, the user should check whether the application offers any option of deactivating active communication channels (for instance SNMP, FTP, BootP, DCP, etc.), or setting passwords to prevent third parties from unauthorized accessing the controller and modifying the system.
3. The access to the devices should be limited to the least possible amount of authorized personal.

4. It is highly recommended to change standard or default passwords when first implementing the component. Passwords should be changed in regular interval in order to reduce risks of becoming public. Passwords should have a maximum strength by the use of small and capital letters as well as numbers and specially characters with a length of at least 10 characters.

5. Regular thread analyses should be conducted to find out whether current measures meet the safety requirements.

6. Installing and permanent maintenance / updates of security software in order to defend new or recurring risks; such as viruses, Trojans, phishing attacks, attracts on networks and other malicious software; is recommended on the computers which are used to program the devices.

In addition to these general recommendations Phoenix Contact is preparing an Update for WebVisit’s password macro mitigating case 1” Password stored and transferred in clear text” which can be used for all ILC 1xx. Customers may contact Phoenix Contact to check when such Update is available. Customers may decide to use the ILC 1x1 PLC’s with latest Firmware 4.42 as they are offering the HTTPS Protocol and HTML5 for the Webserver based HMI system. With regard to the controller's communication interfaces, Phoenix Contact recommend not to use the ILC 1xx controller in safety-critical applications unless using additional security devices. Phoenix Contact is offering such products like the security appliance MGuard, offering VPN and integrated Firewall.

Acknowledgement:
Phoenix Contact would like to thank Matthias Niedermaier and Michael Kapfer of HSASec Hochschule Augsburg and ICS-CERT for a coordinated release of this vulnerability.

Resources:

1. Recommended security practices by ICS-CERT:

http://ics-cert.us-cert.gov/content/recommended-practices

2. Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies

https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

3. For more information about the official ICS-CERT advisory please refer to: https://ics-cert.us-cert.gov/advisories/ICSA-15-013-03

4. For more information about Phoenix Contact's security appliance MGuard, offering VPN and integrated Firewall please refer to: https://www.phoenixcontact.com

For more information contact automation@phoenixcontact.com