Security Advisory Update II
for KUNBUS-GW Modbus TCP PR100088

Overview

The KUNBUS-GW Modbus TCP PR100088 prior to release 03 (software version 1.2.13933) has vulnerabilities regarding its web server.
The vulnerabilities (1-3) were fixed with the software update release 02. The vulnerabilities (1-5) were fixed with the software update release 03.

Products are always delivered with the latest software release.

Affected products

KUNBUS-GW Modbus TCP PR100088, all versions prior to release 03 (software version 1.2.13933).

Vulnerability description

(1) Conditional authentication bypass

This vulnerability allows an attacker to change the password for an administrator user who is currently logged in or who was already logged in without authentication. This void is valid as long as the device was not restarted by a RESET.

CVSS v3 base score of 9.6
CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).

(2) Missing Authentication For Critical Function

This vulnerability allows an attacker to read and write Modbus registers through the web server without proper client authentication.

CVSS v3 base score of 10.0
CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

(3) Denial of Service

This vulnerability allows an attacker to send requests to the embedded FTP server to cause the device to crash if file names longer than 256 characters are used.

CVSS v3 base score of 4.9
CVSS vector string is (AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

KUNBUS GmbH
Heerweg 15C
73770 Denkendorf
Germany
Tel. +49 (0)711 300 20 678
Fax +49 (0)711 300 20 677
Email info@kunbus.de
Web www.kunbus.de

Update 07.02.2019
We have identified following additional vulnerabilities, which were be fixed in release 03

(4) Publication of information by parameter data in an HTTP GET request
This vulnerability allows an attacker to retrieve passwords with an HTTP GET request while in a MITM position.

CVSS v3 base score of 8.8
CVSS vector string is (AV:A/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).

(5) Plain text storage of passwords
This vulnerability allows an attacker to retrieve plain text information stored in an XML file via FTP.

CVSS v3 base score of 7.2
CVSS vector string is (AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).

Countermeasures
Take appropriate measures to protect your network against external access to the gateway.

Please carry out the published software update. We publish security-relevant updates under: https://www.kunbus.com/security-information.html

General safety instructions for KUNBUS gateway products
Please note that the gateway is not suitable for use in unprotected networks (e.g. the Internet). Operate the gateway always in a secure network:

- Protect your network in such a way that no direct access via the Internet is allowed.
- Immediately change the default password of the web server. You will find instructions on how to do this in the user manual.

Check our website regularly for the latest software security alerts and updates for your product. Install the security updates provided by us.

Acknowledgements
KUNBUS would like to thank Nicolas Merle and Applied Risk for finding the vulnerabilities and for their cooperation.

KUNBUS GmbH
Denkendorf,
Place
28.02.2019
Date

Kaufmann, Sandor
Name, First Name
Chief Operating Officer (COO)
Function
Signature

KUNBUS GmbH
Heerweg 15C
73770 Denkendorf
Germany
Tel. +49 (0)711 300 20 678
Fax +49 (0)711 300 20 677
Email info@kunbus.de
Web www.kunbus.de