Update zum Security Advisory für KUNBUS-GW Modbus TCP PR100088

Übersicht

Das KUNBUS-GW Modbus TCP PR100088 vor dem Release 02 (Software-Version 1.1.13166) hat Schwachstellen im Webserver. Die Schwachstellen (1-3) wurden mit dem Software-Update Release 02 beseitigt.

Für die Schwachstellen (4-5) arbeiten wir an einem Software-Update. Mit dem Release 03 werden diese Schwachstellen geschlossen.

Produkte werden immer mit dem neuesten Software-Release ausgeliefert.

Betroffene Produkte

KUNBUS-GW Modbus TCP PR100088, alle Versionen vor Release 02 (Software-Version 1.1.13166).

Schwachstellenbeschreibung

(1) Bedingte Authentifizierungsumgehung

Die Schwachstelle erlaubt einem Angreifer das Passwort für einen Administrator User, welcher aktuell angemeldet ist oder bereits angemeldet war, ohne Authentifizierung zu verändern. Diese Lücke gilt unter der Voraussetzung, dass das Gerät nicht durch ein RESET neu gestartet wurde.

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) Authentifizierungs-Bypass

Die Schwachstelle erlaubt einem Angreifer Modbus Register über den Webserver zu lesen und zu schreiben, ohne dass sich der Client vorher ordnungsgemäß authentifiziert hatte.

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) Diensteverweigerung (Denial of Service)

Die Schwachstelle erlaubt einem Angreifer Anfragen an den integrierten FTP-Server zu schicken, die das Gerät zum Absturz bringen, wenn Dateinamen länger als 256 Zeichen verwendet werden.

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
Deutschland
Tel. +49 (0)711 300 20 678
Fax +49 (0)711 300 20 677
E-mail info@kunbus.de
Web www.kunbus.de

Update 07.02.2019

Folgende zusätzliche Schwachstellen wurden identifiziert und werden mit dem Release 03 behoben.

(4) Informationsveröffentlichung durch Parameterdaten in einem HTTP GET Aufruf

Die Schwachstelle erlaubt einem Angreifer Passwörter mit einem HTTP GET request abzurufen, wenn er sich in einer MITM-Position befindet.

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) Klartext Speicherung von Passwörtern

Diese Schwachstelle erlaubt einem Angreifer über FTP Klartextinformationen abzurufen, die in einer XML-Datei gespeichert sind.

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).

Gegenmaßnahmen

Ergreifen Sie geeignete Maßnahmen, die ihr Netzwerk gegen externe Zugriffe auf das Gateway abschotten.

Bitte führen Sie das veröffentlichte Software-Update durch.
Sicherheitsrelevante Updates veröffentlichen wir unter:
https://www.kunbus.de/produktsicherheit.html

Allgemeine Sicherheitshinweise für KUNBUS Gateway Produkte

Bitte beachten Sie, dass das Gateway nicht zum Einsatz in ungeschützten Netzwerken (z.B. dem Internet) geeignet ist. Betreiben Sie das Gateway in einem gesicherten Netzwerk:

- Schotten Sie Ihr Netzwerk so ab, dass keine direkten Zugriffe über das Internet zugelassen werden.
- Ändern Sie umgehend das Default-Passwort für den Webserver. Eine Anleitung dazu finden Sie im Anwenderhandbuch.
  Hinweis: Wählen Sie ein sicheres neues Passwort. Mehr Informationen dazu finden sie unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

Prüfen Sie regelmäßig auf unserer Website, ob aktuelle Software-Sicherheitswarnungen und Updates für Ihr Produkt vorliegen. Installieren Sie die von uns zur Verfügung gestellten Sicherheitsupdates.

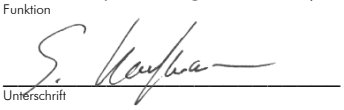
KUNBUS GmbH
Heerweg 15C
73770 Denkendorf
Deutschland
Tel. +49 (0)711 300 20 678
Fax +49 (0)711 300 20 677
E-mail info@kunbus.de
Web www.kunbus.de

Danksagung

KUNBUS bedankt sich bei Nicolas Merle und der Firma Applied Risk für das Auffinden der Schwachstellen und die kooperative Zusammenarbeit.

KUNBUS GmbH
Denkendorf,
Ort
07.02.2019
Datum

Kaufmann, Sandor
Name, Vorname
Chief Operating Officer (COO)
Funktion



Unterschrift

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