

# Security Advisory for Revolution Pi base modules

## Overview

The KUNBUS Revolution Pi web interface prior to web status package version 1.2.12 / 2.0.1 has vulnerabilities regarding its authentication system. The vulnerabilities were fixed with the web status packages 1.2.12 / 2.0.1

Products are always delivered with the latest software release.

## Affected products

Revolution Pi Core/Core3/Core3+/Connect/Connect+/Compact/Flat with installed web status package.

## Vulnerability description

### (1) Username enumeration

This vulnerability allows an attacker to enumerate valid username by observing requests sent to the php/dal.php endpoint.

CVSS v3 base score of 9.6

CVSS vector string

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C

### (2) Authentication Bypass

This vulnerability allows an attacker to access the KUNBUS Revolution Pi web interface without proper client authentication.

CVSS v3 base score of 9.6

CVSS vector string

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C

## General safety instructions for KUNBUS products

- Protect your device with a firewall in case of direct access via the Internet is allowed.
- Update all systems regularly and check log files for suspicious entries.
- 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 Paolo Coba and Nicola Mezzetti for finding the vulnerabilities and for their cooperation.

KUNBUS GmbH

Denkendorf,

Place

03.01.2022


Date

Kaufmann, Sandor

Name, First Name

Chief Operating Officer (COO)

Function



Signature