America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

KUNBUS GmbH Revolution Pi

Release Date: May 01, 2025 **Alert Code:** ICSA-25-121-01

RELATED TOPICS: INDUSTRIAL CONTROL SYSTEM VULNERABILITIES </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, INDUSTRIAL CONTROL SYSTEMS </topics/industrial-control-systems>

View CSAF <https://github.com/cisagov/csaf>

1. EXECUTIVE SUMMARY

- **CVSS v4 9.3**
- **ATTENTION**: Exploitable remotely/low attack complexity
- **Vendor**: KUNBUS
- **Equipment**: Revolution Pi
- **Vulnerabilities**: Missing Authentication for Critical Function, Authentication Bypass by Primary Weakness, Improper Neutralization of Server-Side Includes (SSI) Within a Web Page

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow attackers to bypass authentication, gain unauthorized access to critical functions, and execute malicious server-side includes (SSI) within a web page.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of KUNBUS Revolution Pi are affected:

Revolution Pi OS Bookworm: Versions 01/2025 and earlier
Revolution Pi PiCtory: Versions 2.5.0 through 2.11.1
Revolution Pi PiCtory: Versions 2.11.1 and earlier

3.2 VULNERABILITY OVERVIEW

3.2.1 Missing Authentication for Critical Function CWE-306

<https://cwe.mitre.org/data/definitions/306.html>

KUNBUS Revolution Pi OS Bookworm 01/2025 is vulnerable because authentication is not configured by default for the Node-RED server. This can give an unauthenticated remote attacker full access to the Node-RED server where they can run arbitrary commands on the underlying operating system.

CVE-2025-24522 has been assigned to this vulnerability. A CVSS v3.1 base score of 10.0 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H <https://www.first.org/cvss/calculator/3.1#cvss:3.1/av:n/ac:l/pr:n/ui:n/s:c/c:h/i:h/a:h>).

A CVSS v4 score has also been calculated for CVE-2025-24522. A base score of 9.3 has been calculated; the CVSS vector string is (AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N <https://www.first.org/cvss/calculator/4.0#cvss:4.0/av:n/ac:l/at:n/pr:n/ui:n/vc:h/vi:h/va:h/sc:n/si:n/sa:n>).

3.2.2 Authentication Bypass by Primary Weakness CWE-305 <https://cwe.mitre.org/data/definitions/305.html>

KUNBUS PiCtory versions 2.5.0 through 2.11.1 have an authentication bypass vulnerability where a remote attacker can bypass authentication to get access due to a path traversal.

CVE-2025-32011 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H <https://www.first.org/cvss/calculator/3.1#cvss:3.1/av:n/ac:l/pr:n/ui:n/s:u/c:h/i:h/a:h>).

A CVSS v4 score has also been calculated for CVE-2025-32011. A base score of 9.3 has been calculated; the CVSS vector string is (AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N <https://www.first.org/cvss/calculator/4.0#cvss:4.0/av:n/ac:l/at:n/pr:n/ui:n/vc:h/vi:h/va:h/sc:n/si:n/sa:n>).

3.2.3 Improper Neutralization of Server-Side Includes (SSI) Within a Web Page CWE-97 <https://cwe.mitre.org/data/definitions/97.html>

KUNBUS PiCtory version 2.11.1 and earlier are vulnerable when an authenticated remote attacker crafts a special filename that can be stored by API endpoints. That filename is later transmitted to the client in order to show a list of configuration files. Due to a missing escape or sanitization, the filename could be executed as HTML script tag resulting in a cross-site-scripting attack.

CVE-2025-35996 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.0 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H <https://www.first.org/cvss/calculator/3.1#cvss:3.1/av:n/ac:l/pr:l/ui:r/s:c/c:h/i:h/a:h>).

A CVSS v4 score has also been calculated for CVE-2025-35996. A base score of 8.5 has been calculated; the CVSS vector string is (AV:N/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N <https://www.first.org/cvss/calculator/4.0#cvss:4.0/av:n/ac:l/at:n/pr:l/ui:a/vc:h/vi:h/va:h/sc:n/si:n/sa:n>).

3.2.4 Improper Neutralization of Server-Side Includes (SSI) Within a Web Page CWE-97 <https://cwe.mitre.org/data/definitions/97.html>

KUNBUS PiCtory version 2.11.1 and earlier are vulnerable to a cross-site-scripting attack via the sso_token used for authentication. If an attacker provides the user with a PiCtory URL containing an HTML script as an sso_token, that script will reply to the user and be executed.

CVE-2025-36558 has been assigned to this vulnerability. A CVSS v3.1 base score of 6.1 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N <https://www.first.org/cvss/calculator/3.1#cvss:3.1/av:n/ac:l/pr:n/ui:r/s:c/c:l/i:l/a:n>).

A CVSS v4 score has also been calculated for CVE-2025-36558. A base score of 5.1 has been calculated; the CVSS vector string is (AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N <https://www.first.org/cvss/calculator/4.0#cvss:4.0/av:n/ac:l/at:n/pr:n/ui:a/vc:l/vi:l/va:n/sc:n/si:n/sa:n>).

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Critical Manufacturing, Energy, Transportation Systems, Water and Wastewater Systems
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** Germany

3.4 RESEARCHER

Adam Bromiley of Pen Test Partners reported these vulnerabilities to CISA.

4. MITIGATIONS

KUNBUS has identified the following specific mitigations that users can apply to reduce risk:

- Update PiCtory package to version 2.12

The preferred method for updating to version 2.12 is accomplished through KUNBUS's management UI Cockpit. However, users can also download the update package here <http://packages.revolutionpi.de/pool/main/p/pictory/>.

By end of April 2025, KUNBUS plans to release a new Cockpit plugin that helps the user to make configurations which are available in a graphical interface. In the meantime, it is recommended that users activate authentication. Please refer to this guide <https://www.kunbus.com/files/media/misc/kunbus-2025-0000002-remediation.pdf> for help with activating authentication.

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities, such as:

- Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet <https://www.cisa.gov/uscert/ics/alerts/ics-alert-10-301-01>.
- Locate control system networks and remote devices behind firewalls and isolating them from business networks.
- When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices <https://www.cisa.gov/resources-tools/resources/ics-recommended-practices> on the ICS webpage on cisa.gov/ics <https://www.cisa.gov/topics/industrial-control-systems>. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies <https://us-cert.cisa.gov/sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets <https://www.cisa.gov/sites/default/files/publications/cybersecurity_best_practices_for_industrial_control_systems.pdf>.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics <https://www.cisa.gov/topics/industrial-control-systems> in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies <https://www.cisa.gov/uscert/ics/tips/ics-tip-12-146-01b>.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

No known public exploitation specifically targeting these vulnerabilities has been reported to CISA at this time.

5. UPDATE HISTORY

- May 1, 2025: Initial Publication

Vendor

- Kunbus

Tags

Sector: Critical Manufacturing Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/critical-manufacturing-sector>, Energy Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector>, Transportation Systems Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector>, Water and Wastewater Systems </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/water-and-wastewater-sector>

Topics: Industrial Control System Vulnerabilities </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, Industrial Control Systems </topics/industrial-control-systems>

Related Advisories

APR 29, 2025 ICS ADVISORY | ICSA-25-119-02

Delta Electronics ISPSoft </news-events/ics-advisories/icsa-25-119-02>

APR 29, 2025 ICS ADVISORY | ICSA-25-119-01

Rockwell Automation ThinManager </news-events/ics-advisories/icsa-25-119-01>

APR 24, 2025 ICS ADVISORY | ICSA-25-114-01

Schneider Electric Modicon Controllers </news-events/ics-advisories/icsa-25-114-01>

APR 24, 2025 ICS ADVISORY | ICSA-25-114-02

ALBEDO Telecom Net.Time - PTP/NTP Clock </news-events/ics-advisories/icsa-25-114-02>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CISA Central

1-844-Say-CISA SayCISA@cisa.dhs.gov