KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory "Denial of service vulnerability in components of B&R Industrial Automation GmbH" (KSA-2021-4)

In July 2021, B&R Industrial Automation GmbH published a security advisory that addresses a "Denial of service vulnerability on Automation Runtime webserver" in its products. An attacker, who successfully exploits the vulnerability, may stop the cyclic program on the device and cause a denial of service, according to the B&R advisory.

For the affected products and services, Krones rates the likelihood of being exploited as medium. Therefore, timely action is recommended.

Affected products and services

The following table lists affected products or services, and specific remediation. Krones recommends implementing the suggested remediation measures.

No.	Likelihood of exploitation[1]	Affected products or services	Default state and remediation
1	Medium	Any product that uses affected B&R Automation Runtime prior to 4.7x.	• We recommend implementing the mitigations listed below. • As of Jul 16, 2021, B&R doesn't provide any security updates for these versions.
2	Medium	Any product that uses B&R Automation Runtime from 4.7x to 4.9x.	• We recommend implementing the mitigations listed below. • For Automation Runtime 4.7x to 4.9x, Krones may offer customer-specific updates. Please get in touch with Krones LCS.
Krones may add additional affected products or services, or update remediations as soon as there is new information available.			

Workarounds and mitigations

The following specific workarounds and mitigations are recommended in addition to the remediation measures listed above to further reduce the risk originating from the security vulnerabilities:

- Use firewalls to limit network traffic between the web server on B&R PLCs (TCP port 80) and other networks (e.g., office network, internet). Only allow network traffic that is necessary for your production environment (e.g., MES, data analysis).
- If applicable, monitor your complete network traffic to detect abnormal traffic to TCP port 80.

Security contact

If you have any questions regarding this security advisory or other security-related questions, please contact the Product Security Incident Response Team (PSIRT) of Krones: cyber.security@krones.com

[1] The likelihood of exploitation is rated by Krones for the default Krones use case of the product in its delivery condition. This value may vary in case of customer-specific solutions or changes of the delivery condition.

OpenPGP key for confidential messages:
https://www.krones.com/ext/securitytxt/cyber.security@krones.com.asc

Appendix A: Technical description of the vulnerabilities

This section describes each vulnerability in detail. The CVSS v3.1 base score is the current severity rating according to the original security advisory by B&R and does not necessarily reflect the actual severity in the default Krones environment.

Vulnerability CVE-2021-22275

Improper buffer restrictions in the webserver of Automation Runtime may allow an unauthenticated network-based attacker to stop the cyclic program on the device and cause a denial of service. The vulnerability affects B&R Automation Runtime versions prior to 4.9.1.

The CVSS v3.1 base score for the vulnerability is 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H).

Appendix B: Further information

- B&R Cyber Security Advisory 08/2021 “Denial of service vulnerability on Automation Runtime webserver” - https://www.br-automation.com/en/service/cyber-security/

Appendix C: Changelog

Version	Date	Changes
1.0	2021-07-16	Initial publication by the Krones PSIRT