KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “Denial of service vulnerability in components of B&R Industrial Automation GmbH, July 2023” (KSA-2023-2)

In July 2023, B&R Industrial Automation GmbH released a security advisory on a security vulnerability (“SYN Flooding Vulnerability in Portmapper”) affecting their B&R Automation Runtime software. An attacker, who successfully exploits the vulnerability, can render network services on affected devices unavailable.

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 4.70.	• We recommend implementing the mitigation listed below.
2	Medium	Any product that uses affected B&R Automation Runtime from 4.70 to F4.93.	• We recommend implementing the mitigation listed below. • For customers using Automation Runtime 4.70 or above, 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 mitigation

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

- Use firewalls to limit network traffic between your production lines and other networks (e.g., office network, internet). Only allow network traffic that is necessary for your production environment (e.g., MES, data analysis). In this case, deny network traffic to TCP port 111 of the affected devices.
- If applicable, monitor your complete network traffic to detect abnormal traffic to your production environment, especially network traffic to TCP port 111 of the affected devices.

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

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

[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.

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

Appendix A: Technical description of the security vulnerabilities

This section describes security vulnerabilities covered by this Krones Security Advisory. For each security vulnerability, Krones includes the following public information:

- **Description:** A brief description of the security vulnerability as mentioned in the original security advisory or in the National Vulnerability Database (NVD).
- **CVSS v3.1 Base Score:** The current CVSS v3.1 Base Score as mentioned in the original security advisory or in the National Vulnerability Database (NVD).
- **Listed in CISA Known Exploited Vulnerability Catalog:** Information whether the CISA KEV Catalog lists the security vulnerability. Being listed in the CISA KEV Catalog means that exploitation of the security vulnerability is publicly known. Krones recommends prioritizing handling security vulnerabilities listed in the CISA KEV Catalog.
- **EPSSv3 Score:** The current EPSSv3 Score as available via the FIRST EPSS API. Krones recommends prioritizing handling security vulnerabilities having a high EPSSv3 Score as this may indicate an increased likelihood of being exploited.

Vulnerability CVE-2023-3242

- **Description:** The Portmapper service used in B&R Automation Runtime versions before G4.93 is vulnerable to SYN flooding attacks. An unauthenticated network-based attacker may use this vulnerability to cause several services running on B&R Automation Runtime to become permanently inaccessible.
- **CVSS v3.1 Base Score:** 8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:F/RL:O/RC:C)
- **Listed in CISA Known Exploited Vulnerability Catalog:** No
- **EPSSv3 Score:** 0.000430000

Appendix B: Further information

- Original security advisory by B&R - SYN Flooding Vulnerability in Portmapper (br-automation.com)

Appendix C: Changelog

Version	Date	Changes
1.0	2023-08-09	Initial publication by the Krones PSIRT