KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory "SNMP Authentication and Authorization Weakness in components of B&R Industrial Automation GmbH" (KSA-2020-1)

In February 2020, B&R Industrial Automation GmbH published a security advisory that addresses an "Automation Runtime SNMP Authentication and Authorization Weakness" in its products. SNMP (Simple Network Management Protocol) is a common network protocol for collecting and modifying device information. An attacker, who successfully exploits the vulnerability, can arbitrarily modify the configuration of affected devices, according to the B&R advisory.

For the affected products and services, Krones rates the likelihood of being exploited as low. Therefore, no specific action is required.

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 and services	Default state and remediation
1	Low	Any B&R component that uses B&R Automation Runtime 2.96, 3.00, 3.01, 3.06 to 3.10, 4.00 to 4.63, or 4.72.	As of Mar 4, 2020, B&R doesn't provide any security updates that address the vulnerability. B&R announced that they will disable SNMP by default in future releases.
	Krones may add additional affected products/services, and 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 control SNMP traffic between networks. Explicitly allow SNMP traffic (whitelisting) between hosts. Block SNMP SET commands if you do not use these commands and if blocking commands is supported by your firewall(s).
- If applicable, monitor your complete network traffic to detect anomalous network traffic. In terms of this advisory, SNMP traffic (especially SNMP SET commands) should be detected and analyzed.

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 vulnerability

This section describes each vulnerability in detail. The CVSS v3.0 base score is the current severity rating according to the National Vulnerability Database (NIST) and does not necessarily reflect the actual severity in the default Krones environment.

Vulnerability CVE-2019-19108

CVE-2019-19108 is a vulnerability in the SNMP (Simple Network Management Protocol) service of B&R Automation Runtime. It affects B&R Automation Runtime 2.96, 3.00, 3.01, 3.06 to 3.10, 4.00 to 4.63, or 4.72. An unauthenticated attacker can modify the configuration of affected devices. According to B&R, SNMP credentials can't be changed.

As of Mar 4, 2020, B&R plans to release new versions of B&R Automation Runtime that disable SNMP by default.

The CVSS v3.0 base score for the vulnerability is 9.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H).

Appendix B: Further information

- B&R Cyber Security Advisory 01/2020 "Automation Runtime SNMP Authentication and Authorization Weakness" - https://www.br-automation.com/en/service/cyber-security/

Appendix C: Changelog

Version	Date	Changes
1.0	2020-03-04	Initial publication by the Krones PSIRT