KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “Security vulnerabilities in VC4 Visualization of B&R Industrial Automation GmbH, April 2023” (KSA-2023-1)

In April 2023, B&R Industrial Automation GmbH released a security advisory on three security vulnerabilities affecting their B&R VC4 Visualization software. An attacker, who successfully exploits the vulnerabilities, can bypass the authentication mechanism of the VC4 Visualization, read stack memory, or execute code on affected devices.

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 or services	Default state and remediation
1	Low	Robobox (using Connected HMI, software revisions prior to 69578)	• Krones may offer customer-specific solutions. Please get in touch with Krones LCS. • We recommend implementing the mitigation listed below.
2	None	Robobox (using Zenon HMI)	• By default, Robobox with Zenon HMI doesn’t use B&R VC4 Visualization and is not affected. • No specific action is required.
3	None	Robobox (using Connected HMI, software revision 69578 or newer)	• Revisions 69578 or newer include security updates to address the vulnerabilities. • No specific action is required.
	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 vulnerabilities:

- 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).
- If applicable, monitor your complete network traffic to detect abnormal traffic to your production environment.

[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.

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

Appendix A: Technical description of the vulnerabilities

This section describes the vulnerabilities related to the original security advisory in detail. The CVSS v3.1 base scores are the current severity rating according to the original security advisory or the National Vulnerability Database (NVD) and do not necessarily reflect the actual severity in the default Krones environment.

Vulnerability CVE-2018-20748

LibVNC before 0.9.12 contains multiple heap out-of-bounds write vulnerabilities in libvncclient/rfbproto.c.

The NVD CVSS v3.1 base score for the vulnerability is 9.8
(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C).

Vulnerability CVE-2019-8277

UltraVNC revision 1211 contains multiple memory leaks (CWE-665) in VNC server code, which allows an attacker to read stack memory and can be abused for information disclosure. Combined with another vulnerability, it can be used to leak stack memory and bypass ASLR. This attack appears to be exploitable via network connectivity.

The NVD CVSS v3.1 base score for the vulnerability is 7.5
(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C).

Vulnerability CVE-2023-1617

Improper Authentication vulnerability in B&R Industrial Automation B&R VC4 (VNC-Server modules). This vulnerability may allow an unauthenticated network-based attacker to bypass the authentication mechanism of the VC4 visualization on affected devices. The impact of this vulnerability depends on the functionality provided in the visualization.

The NVD CVSS v3.1 base score for the vulnerability is 9.8
(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C).

Appendix B: Further information

- Original security advisory by B&R - Several Issues in B&R VC4 Visualization (br-automation.com)

Appendix C: Changelog

Version	Date	Changes
1.0	2023-05-09	Initial publication by the Krones PSIRT