KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “Urgent/11 vulnerabilities in components of B&R Industrial Automation GmbH” (KSA-2019-4)

In August 2019, B&R Industrial Automation GmbH published a security advisory that addresses the so-called Urgent/11 security vulnerabilities in its products. Urgent/11 describes 11 security vulnerabilities identified in the real-time operating system VxWorks that is used by embedded systems. B&R Automation Runtime is based on VxWorks, hence it is affected by these security vulnerabilities. An attacker, who successfully exploits the vulnerabilities, can control vulnerable components completely, according to the original Urgent/11 report.

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 B&R Automation Runtime 4.00 – 4.63, available since 2013/2014.	• We primarily recommend implementing the mitigations listed below. • For Automation Runtime 4.1x to 4.6x, Krones may offer customer-specific updates. Please get in touch with Krones LCS.
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 traffic between networks. Explicitly allow traffic (whitelisting). Drop TCP packets that have the Urgent Flag set. Dropping such TCP packets makes it difficult to exploit TCP-based vulnerabilities as described in Urgent/11.
- If applicable, monitor your complete network traffic to detect anomalous network traffic. In case of Urgent/11, TCP packets with the Urgent Flag set, and IP packets with LSRR/SSRR options should be detected and analyzed.

[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 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.

In general, B&R Automation Runtime 2.x and 3.x aren't vulnerable to Urgent/11 according to B&R. For detailed technical description of each vulnerability, see the official URGENT/11 whitepaper (Appendix B: Further information). The following vulnerabilities are part of Urgent/11:

Vulnerability CVE-2019-12255

CVE-2019-12255 is a RCE vulnerability in the TCP layer (TCP Urgent Pointer = 0 leads to integer underflow) of VxWorks. It affects B&R Automation Runtime 4.00 to 4.09.

The CVSS v3.0 base score for the vulnerability is 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

Vulnerability CVE-2019-12256

CVE-2019-12256 is a RCE vulnerability in the IPv4 layer (stack overflow in the parsing of IPv4 packets' IP options) of VxWorks. It affects B&R Automation Runtime 4.10 to 4.63.

The CVSS v3.0 base score for the vulnerability is 9.8 (CVSS:3.0/ AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

Vulnerability CVE-2019-12257

CVE-2019-12257 is a RCE vulnerability (heap overflow in DHCP Offer/ACK parsing inside ipdhcpc) in the IPNet's built-in DHCP client of VxWorks. It affects B&R Automation Runtime 4.00 to 4.09.

The CVSS v3.0 base score for the vulnerability is 8.8 (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

Vulnerability CVE-2019-12258

CVE-2019-12258 can lead to denial of service (DoS; DoS of TCP connection via malformed TCP options) of any TCP connection from/to vulnerable devices. It affects B&R Automation Runtime 4.00 to 4.63.

The CVSS v3.0 base score for the vulnerability is 7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

Vulnerability CVE-2019-12259

CVE-2019-12259 can lead to denial of service (DoS; DoS via NULL dereference in IGMP parsing) by crashing the network stack. It affects B&R Automation Runtime 4.00 to 4.63.

The CVSS v3.0 base score for the vulnerability is 7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

Vulnerability CVE-2019-12260

CVE-2019-12260 is a RCE vulnerability in the TCP layer (TCP Urgent Pointer state confusion caused by malformed TCP AO option) of VxWorks. It affects B&R Automation Runtime 4.10 to 4.63.

The CVSS v3.0 base score for the vulnerability is 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

Vulnerability CVE-2019-12261

CVE-2019-12261 is a RCE vulnerability in the TCP layer (TCP Urgent Pointer state confusion during connect() to a remote host) of VxWorks. It affects B&R Automation Runtime 4.00 to 4.63.

The CVSS v3.0 base score for the vulnerability is 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

Vulnerability CVE-2019-12262

CVE-2019-12262 is a logical error (handling of unsolicited Reverse ARP replies) that can be misused to create invalid routing tables or other routing conflicts. As a result, the vulnerable component can't create any network traffic. It affects B&R Automation Runtime 4.00 to 4.63.

The CVSS v3.0 base score for the vulnerability is 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

Vulnerability CVE-2019-12263

CVE-2019-12263 is a RCE vulnerability in the TCP layer (TCP Urgent Pointer state confusion due to race condition) of VxWorks. It affects B&R Automation Runtime 4.00 to 4.63.

The CVSS v3.0 base score for the vulnerability is 8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).

Vulnerability CVE-2019-12264

CVE-2019-12264 is a logical error (IPv4 assignment by the ipdhcpc DHCP client) that can be misused to assign arbitrary IPv4 addresses. As a result, other attacks are possible. It affects B&R Automation Runtime 4.00 to 4.63.

The CVSS v3.0 base score for the vulnerability is 7.1 (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H).

Vulnerability CVE-2019-12265

CVE-2019-12265 is an information leak (IGMP Information leak via IGMPv3 specific membership report). It affects B&R Automation Runtime 4.00 to 4.63.

The CVSS v3.0 base score for the vulnerability is 5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).

Appendix B: Further information

- URGENT/11 Whitepaper - Critical vulnerabilities to remotely compromise VxWorks, the most popular RTOS - https://go.armis.com/urgent11
- B&R Cyber Security Advisory 01/2019 "Information regarding Wind River VxWorks IPnet Vulnerabilities" - https://www.br-automation.com/de/service/cyber-security/

Appendix C: Changelog

Version	Date	Changes
1.0	2019-10-17	Initial publication by the Krones PSIRT
1.1	2020-04-08	Added information on updates for B&R Automation Runtime versions.