KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “Ripple20 vulnerabilities” (KSA-2020-2)

In June 2020, the JSOF research lab published a report about 19 security vulnerabilities in the network stack of Treck, Inc. These security vulnerabilities are commonly known as “Ripple20”. Ripple20 affects a large set of diverse components from different vendors. An attacker, who successfully exploits the vulnerabilities, can arbitrarily execute code, access information that is normally inaccessible, or trigger errors.

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	Krones machines that contain Rockwell PLCs (using the Rockwell 1734-AENT/R Series B and Series C Ethernet/IP adapter; affected by 6 vulnerabilities)	• By default, the affected adapter is only connected to the isolated internal machine network. • Keep the internal machine network isolated from other networks.
2	Low	PCS systems (BOTEC) (using the Schneider Electric AP9630 UPS NMC2; affected by 15 vulnerabilities)	• By default, the affected network management card is only connected to the isolated BOTEC network. • Keep the BOTEC network isolated.
3	Low	PCS systems (BOTEC) (using the HPE iLO 5; affected by 8 vulnerabilities)	• By default, the affected firmware is only exposed to the isolated BOTEC network. • Keep the BOTEC network isolated. • 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 control traffic between IT/OT networks and production lines. Explicitly allow traffic (whitelisting). If applicable, reject IP fragmented packets, IP tunneling (IPv6-in-IPv4, and IP-in-IP), IP

[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.

source routing, IPv6 deprecated features, malformed TCP packets, unused ICMP control messages, and IPv6 multicast.

- If applicable, monitor your complete OT network traffic to detect anomalous network traffic. In terms of this advisory, IP-in-IP traffic with IP fragments 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

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 National Vulnerability Database (NIST) and does not necessarily reflect the actual severity in the default Krones environment.

Vulnerability CVE-2020-11896

The Treck TCP/IP stack before 6.0.1.66 allows remote code execution, related to IPv4 tunneling. Improper handling of length parameter inconsistency in IPv4/UDP component when handling a packet sent by an unauthorized network attacker.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

According to HP Enterprise Development, the HPE Integrated Lights-Out 5 (iLO 5) is affected by this vulnerability (Last update by HPE: July 13, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

Vulnerability CVE-2020-11897

The Treck TCP/IP stack before 5.0.1.35 has an out-of-bounds write via multiple malformed IPv6 packets. Improper handling of length parameter inconsistency in IPv6 component when handling a packet sent by an unauthorized network attacker.

The CVSS v3.1 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

Vulnerability CVE-2020-11898

The Treck TCP/IP stack before 6.0.1.66 improperly handles an IPv4/ICMPv4 length parameter inconsistency, which might allow remote attackers to trigger an information leak.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

According to HP Enterprise Development, the HPE Integrated Lights-Out 5 (iLO 5) is affected by this vulnerability (Last update by HPE: July 13, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 9.1 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H).

Vulnerability CVE-2020-11899

The Treck TCP/IP stack before 6.0.1.66 has an IPv6 out-of-bounds read. Improper input validation in IPv6 component when handling a packet sent by an unauthorized network attacker.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 5.4 (AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).

Vulnerability CVE-2020-11900

The Treck TCP/IP stack before 6.0.1.41 has an IPv4 tunneling double free. This vulnerability may result in use after free.

According to HP Enterprise Development, the HPE Integrated Lights-Out 5 (iLO 5) is affected by this vulnerability (Last update by HPE: July 13, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H).

Vulnerability CVE-2020-11901

The Treck TCP/IP stack before 6.0.1.66 allows remote code execution via a single invalid DNS response.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

According to Rockwell Automation, the Rockwell 1734-AENT/R Series B and C Ethernet/IP adapter is affected by this vulnerability (Last update by RA: June 16, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in the internal machine network that is isolated from other networks by default (e.g., the line network).

The CVSS v3.1 base score for the vulnerability is 9.0 (AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).

Vulnerability CVE-2020-11902

The Treck TCP/IP stack before 6.0.1.66 has an IPv6OverIPv4 tunneling out-of-bounds read. Improper input validation in IPv6 over IPv4 tunneling component when handling a packet sent by an unauthorized network attacker.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 7.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).

Vulnerability CVE-2020-11903

The Treck TCP/IP stack before 6.0.1.28 has a DHCP out-of-bounds read.

The CVSS v3.1 base score for the vulnerability is 6.5 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

Vulnerability CVE-2020-11904

The Treck TCP/IP stack before 6.0.1.66 has an integer overflow during memory allocation that causes an out-of-bounds write. Possible integer overflow or wraparound in memory allocation component when handling a packet sent by an unauthorized network attacker.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 7.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).

Vulnerability CVE-2020-11905

The Treck TCP/IP stack before 6.0.1.66 has a DHCPv6 out-of-bounds read.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 6.5 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

Vulnerability CVE-2020-11906

The Treck TCP/IP stack before 6.0.1.66 has an Ethernet link layer integer underflow.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

According to Rockwell Automation, the Rockwell 1734-AENT/R Series B and C Ethernet/IP adapter is affected by this vulnerability (Last update by RA: June 16, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in the internal machine network that is isolated from other networks by default (e.g., the line network).

According to HP Enterprise Development, the HPE Integrated Lights-Out 5 (iLO 5) is affected by this vulnerability (Last update by HPE: July 13, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 6.3 (AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).

Vulnerability CVE-2020-11907

The Treck TCP/IP stack before 6.0.1.66 improperly handles a length parameter inconsistency in TCP.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

According to Rockwell Automation, the Rockwell 1734-AENT/R Series B and C Ethernet/IP adapter is affected by this vulnerability (Last update by RA: June 16, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in the internal machine network that is isolated from other networks by default (e.g., the line network).

According to HP Enterprise Development, the HPE Integrated Lights-Out 5 (iLO 5) is affected by this vulnerability (Last update by HPE: July 13, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 6.3 (AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).

Vulnerability CVE-2020-11908

The Treck TCP/IP stack before 4.7.1.27 mishandles '\0' termination in DHCP. This vulnerability may allow exposure of sensitive information.

The CVSS v3.1 base score for the vulnerability is 4.3 (AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).

Vulnerability CVE-2020-11909

The Treck TCP/IP stack before 6.0.1.66 has an IPv4 integer underflow.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).

Vulnerability CVE-2020-11910

The Treck TCP/IP stack before 6.0.1.66 has an ICMPv4 out-of-bounds read. Improper input validation in ICMPv4 component when handling a packet sent by an unauthorized network attacker.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

According to Rockwell Automation, the Rockwell 1734-AENT/R Series B and C Ethernet/IP adapter is affected by this vulnerability (Last update by RA: June 16, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in the internal machine network that is isolated from other networks by default (e.g., the line network).

The CVSS v3.1 base score for the vulnerability is 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).

Vulnerability CVE-2020-11911

The Treck TCP/IP stack before 6.0.1.66 has improper ICMPv4 access control, which may allow an attacker to change one specific configuration value.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

According to Rockwell Automation, the Rockwell 1734-AENT/R Series B and C Ethernet/IP adapter is affected by this vulnerability (Last update by RA: June 16, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in the internal machine network that is isolated from other networks by default (e.g., the line network).

According to HP Enterprise Development, the HPE Integrated Lights-Out 5 (iLO 5) is affected by this vulnerability (Last update by HPE: July 13, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).

Vulnerability CVE-2020-11912

The Treck TCP/IP stack before 6.0.1.66 has a TCP out-of-bounds read. Improper input validation in TCP component when handling a packet sent by an unauthorized network attacker.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

According to Rockwell Automation, the Rockwell 1734-AENT/R Series B and C Ethernet/IP adapter is affected by this vulnerability (Last update by RA: June 16, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in the internal machine network that is isolated from other networks by default (e.g., the line network).

According to HP Enterprise Development, the HPE Integrated Lights-Out 5 (iLO 5) is affected by this vulnerability (Last update by HPE: July 13, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).

Vulnerability CVE-2020-11913

The Treck TCP/IP stack before 6.0.1.66 has an IPv6 out-of-bounds read.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).

Vulnerability CVE-2020-11914

The Treck TCP/IP stack before 6.0.1.66 has an ARP out-of-bounds read.

According to Schneider Electric, the AP9630 UPS NMC2 is affected by this vulnerability (Last update by SE: June 23, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

According to HP Enterprise Development, the HPE Integrated Lights-Out 5 (iLO 5) is affected by this vulnerability (Last update by HPE: July 13, 2020). Krones rates the likelihood of being exploited as low since the affected component is only used in an isolated network.

The CVSS v3.1 base score for the vulnerability is 4.3 (AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).

Appendix B: Further information

- JSOF "19 Zero-Day Vulnerabilities Amplified by the Supply Chain" - https://www.jsof-tech.com/ripple20/
- CISA "ICS Advisory (ICSA-20-168-01)" - https://www.us-cert.gov/ics/advisories/icsa-20-168-01
- CERT/CC "Treck IP stacks contain multiple vulnerabilities" - https://kb.cert.org/vuls/id/257161

Appendix C: Changelog

Version	Date	Changes
1.0	2020-07-09	Initial publication by the Krones PSIRT
1.1	2020-07-29	Added "HPE iLO5" to affected components