Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
-
Phone number
+49 451 882-6166

E-mail
hannes.molsen@draeger.com
fabian.busch@draeger.com
matt.mckenna@draeger.com

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory

URGENT/11 WindRiver VxWorks Security Advisory for multiple network-stack vulnerabilities

>> Certain Dräger Medical Devices are running on vulnerable VxWorks versions and are therefore affected by the several of the vulnerabilities.

Legal Notice

This Product Security Advisory is based on all our findings that we had at the time of publication. However, the facts of the case are being reviewed on an ongoing basis and it is possible that this may result in changed assessments or that assessments contained in this advisory may turn out to be incorrect. We also reserve the right to change or revoke any recommendations. In addition, differences may result from the circumstances of the individual case on site. This information is naturally not available to us and has not been taken into account. Dräger can therefore accept no responsibility that the information presented here is conclusive or comprehensively correct for you. Therefore, please check carefully to what extent deviations can arise for your individual case. If necessary, you will be informed about new findings through following advisories.

1 Publication Date

2019-07-29

2 Overview

In a coordinated vulnerability disclosure process WindRiver published information regarding eleven security vulnerabilities (also known as “URGENT/11”) found in the network stack of the widely used embedded operating system VxWorks.

At Dräger, your cybersecurity is our priority, which is why the product security team immediately verified which Dräger products are affected by the aforementioned vulnerabilities and together with the product risk managers assessed the risk towards patient safety.

Some of our medical devices are running vulnerable versions of the operating system, therefore it is crucial to read this information carefully to identify whether your medical devices are affected, what are the risks associated with the vulnerabilities, and what you can do until a patch is installed on your systems.

Customers of affected products which need to take action are notified separately via a dedicated customer information.
In the following we will describe each vulnerability and the possible impact on an affected device.

The full text of this advisory can be accessed through https://static.draeger.com/security.
WindRiver published a security advisory on https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/

3 Affected Products

The following Dräger devices are affected by these vulnerabilities:

Device	Affected software version	Vulner-abilities exploit-able	Device can still be used	Short-Term measures required	Software patch required
Evita V300	up to SW 2.51	No	Yes	No	No
Infinity Acute Care System – Workstation Critical Care (Evita Infinity V500)		No	Yes	No	No
Infinity Acute Care System – Workstation Neonatal Care (Babylog VN500)		No	Yes	No	No
Babyleo TN500	up to SW 1.04	Yes	Yes	No	Yes
Perseus A500	SW 1.1n up to SW 1.13 SP1 SW 2.0n up to SW 2.02	Yes	Yes	Yes	Yes
Connectivity Converter CC300	SW 1.1	Yes	Yes	Yes	Yes

All other Dräger products and software versions are ***not affected*** by these vulnerabilities, because they either do not contain the vulnerable operating system, or – like the Atlan A300 / Atlan A350 - have been patched before the devices have been shipped to customers.

4 How to verify if the product is affected

All software versions of the previously specified products are affected. In the following we will describe how the currently installed software version of the individual devices can be identified

4.1 Perseus A500

In Standby-Mode go to **System Setup > System Status** to view the installed software version

4.2 Babyleo TN500

Go to **System Setup > System > Service** (User Password required) to view the installed software version

4.3 Evita V300 / Infinity Acute Care System – Workstation Critical Care (Evita Infinity V500) / Infinity Acute Care System – Workstation Neonatal Care (Babylog VN500)

Go to **System Setup > System** to view the installed software version. The information is also displayed on the splash-screen during system boot.

4.4 Connectivity Converter CC300

The CC300 is a headless unit without user interface. The software version can be read by a service technician.

5 Vulnerability Description

The Vulnerabilities are listed under 11 different CVE identifiers and were CVSS rated by WindRiver according to the following table:

CVE ID	Affected Component	CVSSv3	Description
CVE-2019-12256	IPv4	9.8	Stack overflow in the parsing of IPv4 packets IP options
CVE-2019-12257	DHCP Client	8.8	Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc
CVE-2019-12255	TCP	9.8	TCP Urgent Pointer = 0 leads to integer underflow
CVE-2019-12260	TCP	9.8	TCP Urgent Pointer state confusion caused by malformed TCP AO option
CVE-2019-12261	TCP	8.8	TCP Urgent Pointer state confusion during connect() to a remote host
CVE-2019-12263	TCP	8.1	TCP Urgent Pointer state confusion due to race condition
CVE-2019-12258	TCP	7.5	DoS of TCP connection via malformed TCP options
CVE-2019-12259	IPv4 / IGMP	6.3	DoS via NULL dereference in IGMP parsing
CVE-2019-12262	ARP	7.1	Handling of unsolicited Reverse ARP replies (Logical Flaw)
CVE-2019-12264	DHCP Client	7.1	Logical flaw in IPv4 assignment by the ipdhcpc DHCP client
CVE-2019-12265	IPv4 / IGMP	5.4	IGMP Information leak via IGMPv3 specific membership report

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Stefan Lauer
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner

6 Impact

Not all vulnerabilities affect all products. In the following section we will describe in detail how each of the affected products is affected by which vulnerability.

6.1 Perseus A500

The intended use of the Perseus A500 network interface allows the device to be permanently connected to a network to offer features like time synchronization. Furthermore the network interface is used for service purposes, like installing new device software. Unauthenticated remote attackers on the same network can exploit these vulnerabilities.

CVE ID	Affected	Impact
CVE-2019-12256	No	The vulnerability does not affect the used version of VxWorks.
CVE-2019-12257	Yes	A spoofed DHCP response (Offer/ACK) can cause Remote-Code-Execution or Denial of Service of the affected device.
CVE-2019-12255 **CVE-2019-12260** **CVE-2019-12261** **CVE-2019-12263**	Yes	Specifically crafted TCP Packets with the Urgent Flag set can cause a memory corruption and thereby possibly a Denial of Service of the affected device.
CVE-2019-12258	No	The vulnerability affects only TCP servers, the device can only act as a TCP client.
CVE-2019-12259	No	The device does not use IGMP in the affected way.
CVE-2019-12265	Yes	The vulnerability allows an attacker to extract data from previously sent/received packets
CVE-2019-12262	Yes	The vulnerability allows an attacker on the same subnet to set additional IP addresses that the device listens to.
CVE-2019-12264	Yes	A spoofed DHCP response can lead to an invalid IP address being assigned to the device

6.2 Babyleo TN500

The intended use of the Babyleo TN500 network interface **does not allow** the device to be connected to a network. The interface is solely to be used for local service purposes using a point-to-point cross cable. The IP address of the device is static and can't be changed. Therefore, to be able to exploit these vulnerabilities, an attacker would need to have physical access to the device, or the unlikely circumstance that the device is connected to a network against its intended use with an IP subnet matching the static IP address of the device.

CVE ID	Affected	Impact
CVE-2019-12256	No	The vulnerability does not affect the used version of VxWorks.
CVE-2019-12257 **CVE-2019-12264**	No	A DHCP client is not running on the device
CVE-2019-12255 **CVE-2019-12260** **CVE-2019-12261** **CVE-2019-12263**	Yes	Specifically crafted TCP Packets with the Urgent Flag set can cause a memory corruption and thereby possibly a Denial of Service of the affected device.
CVE-2019-12258	No	The vulnerability affects only TCP servers, the device can only act as a TCP client.
CVE-2019-12259	No	The device does not use IGMP in the affected way.
CVE-2019-12265	Yes	The vulnerability allows an attacker to extract data from previously sent/received packets
CVE-2019-12262	Yes	The vulnerability allows an attacker on the same subnet to set additional IP addresses that the device listens to.

6.3 Evita V300 / Infinity Acute Care System – Workstation Critical Care (Evita Infinity V500) / Infinity Acute Care System – Workstation Neonatal Care (Babylog VN500)

This is a system consisting of two components: the display and user interface unit, which we call the “cockpit”, and the ventilation unit. Only the ventilation unit is running the vulnerable operating system, the service network interface is located on the cockpit and therefore not affected by these vulnerabilities.
The network interface of the ventilation unit is not to be used, neither by customers, nor by service. In order to avoid accidental connections, it is only accessible with a proprietary cable. Furthermore, the IP address of the ventilation unit is static and can’t be changed.

CVE ID	Affected	Impact
CVE-2019-12256	No	The vulnerability does not affect the used version of VxWorks.
CVE-2019-12257 **CVE-2019-12264**	No	A DHCP client is not running on the device
CVE-2019-12255 **CVE-2019-12260** **CVE-2019-12261** **CVE-2019-12263**	Yes	Specifically crafted TCP Packets with the Urgent Flag set can cause a memory corruption and thereby possibly a Denial of Service of the affected device.
CVE-2019-12258	No	The vulnerability affects only TCP servers, the device can only act as a TCP client.
CVE-2019-12259	No	The device does not use IGMP in the affected way.
CVE-2019-12265	Yes	The vulnerability allows an attacker to extract data from previously sent/received packets
CVE-2019-12262	Yes	The vulnerability allows an attacker on the same subnet to set additional IP addresses that the device listens to.

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Stefan Lauer
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner

6.4 Connectivity Converter CC300

The Connectivity Converter CC300 software 1.1 may be connected to the serial ports of the following devices:

- Perseus A500
- Primus
- Primus IE
- Infinity Acute Care System – Workstation Critical Care (Evita Infinity V500)
- Evita V300
- Infinity Acute Care System – Workstation Neonatal Care (Babylog VN500)

The CC300 network interface allows the device to be permanently connected to a network to offer system functionality like time synchronization, data export and remote alarm silence.

CVE ID	Affected	Impact
CVE-2019-12256	Yes	A spoofed IP packet with invalid IP options can cause Remote-Code-Execution or Denial of Service of the affected device.
CVE-2019-12257	No	The vulnerability does not affect the used version of VxWorks.
CVE-2019-12255	No	The vulnerability does not affect the used version of VxWorks.
CVE-2019-12260 **CVE-2019-12261** **CVE-2019-12263**	Yes	Specifically crafted TCP Packets with the Urgent Flag set can cause a memory corruption and thereby possibly a Denial of Service of the affected device.
CVE-2019-12258	Yes	A malformed packet can cause a TCP connection to be closed by an attacker on the same network.
CVE-2019-12259	No	The device does not use IGMP in the affected way.
CVE-2019-12265	Yes	The vulnerability allows an attacker to extract data from previously sent/received packets
CVE-2019-12262	Yes	The vulnerability allows an attacker on the same subnet to set additional IP addresses that the device listens to.
CVE-2019-12264	Yes	A spoofed DHCP response can lead to an invalid IP address being assigned to the device

7 Severity

The WindRiver provided CVSSv3 Scores for the vulnerabilities are listed in the table in chapter 5.
Note that the Impact of the CVSSv3 is focused on the affected component alone and is **not directly linkable to a risk to patient safety.** The risk to patient safety of the vulnerabilities can be assessed only taking into consideration the intended use of the network interfaces to determine a likelihood of exploitation. This needs to be taken into consideration together with the probability that a successful exploitation then leads to harm.

7.1 Perseus A500

The risk towards patient safety is considered to be low. The most likely result of a successful exploitation is a loss of network functionality or potentially a device reboot. It is unlikely that an exploitation of this vulnerability leads to patient harm, as the anesthesia device is permanently attended by a physician. Nevertheless, as a preventive measure, we recommend to unplug the device from the network until the patch is installed on the system.

7.2 Babyleo TN500

The security vulnerabilities pose no risk towards patient safety, as the network interface must not be connected to a network during therapy, and therefore the vulnerabilities can't be exploited.

7.3 Evita V300 / Infinity Acute Care System – Workstation Critical Care (Evita Infinity V500) / Infinity Acute Care System – Workstation Neonatal Care (Babylog VN500)

The security vulnerabilities pose no risk towards patient safety, as the affected network interface is not functional without a proprietary cable and must not be connected to a network. Therefore the vulnerabilities can't be exploited.

7.4 Connectivity Converter CC300

The risk towards patient safety is considered to be low. The most likely result of a successful exploitation is a loss of network functionality or potentially a device reboot. It is unlikely that an exploitation of this vulnerability leads to patient harm, as the affected component is not the connected therapy device. A successful exploitation might lead to a loss of system functionality. Nevertheless, as a preventive measure, we recommend to unplug the device from the network until the patch is installed on the system.

8 Remediation

Customers can continue to use the affected devices, the therapeutic functions are not affected by these vulnerabilities. However, as a preventive measure, we recommend customers to take further action for some of the affected devices:

8.1 Perseus A500

The device needs to be unplugged from the network until the patch is installed on the device.
The patched version 1.14 is planned to be available in Q3/2019
The patched version 2.03 is planned to be available in Q4/2019.

8.2 Babyleo TN500

The device must not be connected to a network.
The patched version 1.05 is planned to be available in Q3/2019.

8.3 Evita V300 / Infinity Acute Care System – Workstation Critical Care (Evita Infinity V500) / Infinity Acute Care System – Workstation Neonatal Care (Babylog VN500)

The device's ventilation unit must not be connected to a network.

8.4 Connectivity Converter CC300

The device must be unplugged from the network until the patch is installed on the device.
The patched version 1.11 is available since 2019-07-30.

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Stefan Lauer
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner

9 Contact Information

If you have any further questions related to the impact of the vulnerabilities, please contact your designated regional marketing manager. For reporting incidents and potential vulnerabilities in our devices, please refer to https://static.draeger.com/security to contact the Product Security team directly.

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Stefan Lauer
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner

Revisions

Version	Date	Change
1	2019-07-29	Initial Document
2	2019-07-29	Added WindRiver Advisory-Link and URGENT/11 as the name
3	2019-07-31	CC300 SW is available

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Stefan Lauer
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner