Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
-
Phone number
+49 451 882-6166

E-mail
hannes.molsen@draeger.com
detlef.koeble@draeger.com
matt.mckenna@draeger.com

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-20-169-01

Perseus A500 SW 2.0n Security 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

2020-06-17

2 Overview

Dräger has become aware of isolated cases in which the Medibus interface of the Perseus A500 was disrupted by external non-Medibus-compliant data packages such that the internal processor became overloaded. This resulted in delays to the display of ventilation curves on the screen of the Perseus, and subsequently the devices in question performed warm starts. As a result, the ventilation pressure dropped and ventilation was interrupted for a few seconds before therapy was resumed with the same settings as before.

The full text of this advisory can be accessed through https://static.draeger.com/security.

3 Affected Products

The following Dräger devices are affected by these vulnerabilities:

Dräger Perseus A500, software versions 2.00 up to and including 2.02.

4 How to verify if the product is affected

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

5 Vulnerability Description

CWE-20: Improper Input Validation
Perseus does not handle certain specifically crafted non-Medibus-compliant data via the Medibus interface properly.

6 Impact

The display of curves may be delayed and ultimately a warm start may be performed. When controlled ventilation modes are being used, a warm start causes the ventilation pressure to fall to the ambient level. This could possibly result in a deterioration of the patient's condition.

7 Severity

The severity may be different in certain use environments. The intended connection of the RS-232 interface is a point-to-point connection, leading to an attack vector "local", but in certain environments this serial connection is routed over ethernet using third party off-the-shelf converters. This may then lead to a higher score, as the attack vector can also be "network".

The CVSSv3.1 Scores for the vulnerability are:

1. *Denial of Service via RS-232:* **Base Score 3.2 (LOW)**
   CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:L
2. *Denial of Service via RS-232 routed via Ethernet:* ***Base Score 4.0 (MEDIUM)***
   CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:L

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

8 Remediation

The vulnerability has been fixed in software version SW 2.03. Customers will be contacted by Dräger Service to arrange a date for the software to be updated free of charge.

Until then, customers may choose to mitigate the risk in one of the following ways:

Alternative 1:
Do not use the Medibus interface until the improved software has been installed on your devices.

Alternative 2:
If there are important reasons why you are unable to do without the Medibus interface even for a transitional period, please watch very carefully to see how the curves are displayed and compare them to the inflating manual ventilation bag.
If you notice that the curves are only being displayed with some delay, disconnect the Medibus interface and carry out a controlled reboot of the Perseus by switching off the device and then switching it on again. During this time you can manually ventilate the patient using the O2 emergency flow control, the Vapor and the manual ventilation bag. The interface should then remain disconnected until the possibility of non-Medibus-compliant data being supplied can be completed ruled out.
If you are actively using the Medibus interface of your Perseus at the current time or plan to do so in the near future, please contact your local Dräger representative so that we can take this into account when planning the software updates.
The non-Medibus-compliant data in question can be caused by defective components or settings in the network.

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

10 Revision History

VERSION	DATE	COMMENTS
1.0	2020-06-17	Initial Advisory Release

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