Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
-
Phone number
+49 451 882-6166

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-19-255-02

Infinity® Acute Care System and M540 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

Initial: 2019-09-12

Update: 2021-10-19

2 Overview

Several Cybersecurity vulnerabilities have been discovered in the Dräger Infinity Acute Care System™ and the Standalone Infinity® M540 patient monitors (software version VG4.1.1/VG4.0.3 and lower) which may cause the device to reboot and/or lose functionality.

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 Infinity Acute Care System software version VG4.1.1/VG4.0.3 and lower
- Dräger Standalone Infinity M540 patient monitor software version VG4.1.1 and lower

4 How to verify if the product is affected

On the M540 go to **Menu > System setup > System information** and review the **S/W revision**

5 Vulnerability Description

1. **Spoofed and Tampered Data**
   Data sent by the M540 or Cockpit is compromised
   Data received by the M540 or Cockpit is compromised

2. **Distributed Denial of Service (DDoS)**
   Quantity of incoming data overwhelms system.

6 Impact

1. **Disclosure of Data**

   Spoofing or tampering can compromise data sent by an M540 or Cockpit which would affect network consumers of monitor data. If this were to occur, the M540 will maintain essential performance (continue to display real-time waveform data and vital sign information on the display as well as initiate physiological and technical alarms). The port on the switch connected to the physical access point would also have to be enabled

2. **Possible to modify device settings**

   Spoofing or tampering can compromise data received by an M540 or Cockpit in other ways as well. If this were to occur, the M540 continues to display real-time patient waveform and vital sign information on the display. However, if the M540 is configured to accept remote control from the Infinity Central Station (ICS) the alarms could be turned OFF or the alarm limits modified. If heart rate and arrhythmia alarms are turned off, a banner is displayed on the M540 and remotely on the ICS to indicate that the alarms are disabled. In addition, the alarm status icon in the vital sign parameter box is updated to indicate alarms are disabled. The port on the switch connected to the physical access point would also have to be enabled.

3. **Denial of Service (DDoS)**

   During a DDoS, the wired Infinity Network may be compromised causing the Cockpit to reboot. The Infinity Acute Care System will no longer be connected to the network. The M540, however will maintain essential performance (continue to display real-time waveform data and vital sign information on the display as well as initiate physiological and technical alarms). Because the

device is no longer on the network, the M540 alarm volume will increase to 100% and the network alarms will annunciate to indicate that the M540 is no longer connected to the cockpit and Infinity Network. The attacker would need to have physical access to a dedicated Infinity network port that is enabled by the IT department.

A DDoS can also occur when the M540 is connected to a wireless network. This can cause the M540 to reboot. If wireless option is enabled, wireless functionality is only utilized while the M540 device is on transport. Wireless is disabled upon docking to the M500 standalone or the IACS configuration. The attacker would need to have physical proximity to an Infinity network access point that is enabled by the IT department.

7 Severity

CVSS 3.1 Score

Base Score: 8.6

Severity: High

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

8 Remediation

For customers who currently have Infinity Acute Care System or M540 patient monitor, VG4.1.1/VG4.0.3 or lower software releases of the affected components can be upgrade to Infinity Acute Care System VG4.2 and Standalone M540 patient monitors to VG4.2 software release. The software is currently available on Draeger ServiceConnect. The fix contains the following improvements:

1. *Distributed Denial of Service (DDoS)* Improve the M540 software by detecting application messages that are too big and employing queue flood management in the software.
2. *Tampering* Update the M540 software by implementation of protocol validation of malformed ACS messages.

We recommend that you follow best recommended practices to limit access to the Infinity Network by assigning separate VLANs and protecting the network by setting up firewalls.

For questions about your specific installation please contact your local Dräger Service Representative.

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	2019-09-12	Initial Document
2	2021-10-19	Update CVSS score and added VG4.2 as the fixed software version

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