Dräger

Urgent - Medical Device Recall

Notice of cybersecurity vulnerabilities for

The Infinity® Acute Care System™ (IACS) and the Standalone Infinity® M540 patient monitor; software version VG4.1.1/VG4.0.3 and lower.

September 13, 2019

Dear Directors of the Biomedical Department, Information Systems, or Risk Management:

The purpose of this letter is to advise you that Dräger is voluntarily recalling our Infinity Acute Care System and the Standalone Infinity M540 patient monitors due to cybersecurity vulnerabilities. These vulnerabilities may cause your device to reboot, lose alarm functionality, and/or lose communication with the cockpit and/or the Infinity Network.

The cybersecurity vulnerabilities can include Distributed Denial of Service (DDoS) (packet storm), Spoofing, and Tampering. The device impacts are described as follows:

During a Distributed Denial of Service (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 Infinity 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 your IT department.

A Distributed Denial of Service (DDoS) can also occur when the M540 is connected to a wireless network. This can cause the M540 to reboot. The M540 reboots within 45 seconds. All alarm settings are maintained. If the wireless option is enabled, wireless functionality is only utilized while the M540 device is on transport. The wireless option 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 your IT department.

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 attacker would need to have physical proximity to an Infinity network access point that is enabled by your IT department.

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 attacker would need to have physical proximity to an Infinity network access point that is enabled by your IT department.

A device failure due to these vulnerabilities could potentially result in delayed intervention or lack of patient monitoring. To date, Dräger has received no reports of harm associated with these vulnerabilities.

The disclosure of the vulnerabilities is published via a US-CERT site and can be located via the following links:
https://www.us-cert.gov/ics/advisories
https://static.draeger.com/security

To mitigate these cybersecurity concerns, Dräger will be releasing software version VG4.2 for both the Cockpit and the M540, which will correct those cybersecurity vulnerabilities. The software is expected to be released for distribution in December 2019. Upgrades of the IACS systems will commence in January 2020.

While we are in the process of updating the software, we recommend that you follow best recommended practices to limit access to the Infinity Network by following these security recommendations:

- Physical security of the patient monitors is recommended and is the responsibility of the operating organization.
- Physical security of the telecommunications closet is recommended and is the responsibility of the operating organization.
- Dräger recommends that operating organizations restrict physical access to unused Ethernet ports on the IACS.
- Dräger recommends that operating organizations restrict physical access to unused USB and serial ports on the IACS.
- Dräger relies on the medical device isolation mechanism of the VLANs and the proper configuration, implementation, and use of the operating organization's security measures to prevent the introduction of malware onto the Infinity Network.

Please complete the attached Acknowledgement and Response Form and return it to Dräger per instructions included on the form. Your local Dräger Service Representative will contact you to schedule an appointment to upgrade your system(s) software free of charge once the new software version is released for distribution.

If you are aware of any incidents related to this issue or if you have any further questions regarding operation of your patient monitor, please contact Dräger Service Technical Support between the hours of 8:00 AM – 8:00 PM EST at 1-800-437-2437 (press 2 at the prompt, then 2, then 1).

Adverse events or quality problems experienced with the use of this product may be reported to FDA's MedWatch Adverse Event Reporting program either online or by phone at 1-800-FDA-1088.

If you have any questions regarding this letter, please contact Michael Kelhart between the hours of 8:00 AM – 4:30 PM EST at 1-800-437-2437 (press 1 at the prompt, then 32349).

Thank you for your understanding and continued support.

Sincerely yours,

Lloyd Stern
Vice President of Product Management
Dräger Patient Monitoring Systems

Dräger

Customer Acknowledgement and Response Form

Please complete this form in its entirety

Cybersecurity vulnerabilites for the Infinity® Acute Care System™ and the standalone Infinity® M540 patient monitor, software version VG4.1.1/VG4.0.3 and lower, all serial numbers.

Customer Name/Address:

_____

_____

_____

☐ I acknowledge the receipt of the information in the attached notice

If this product is no longer in use, please let us know

☐ This product was removed from service and is no longer in use

☐ I have reviewed this information and I do not wish to upgrade our products at this time

Completed By:

Print Name: _____

Telephone _____ Email: _____

Signature: _____

Date: _____

Please forward the completed form to Dräger via fax 215-372-2940 or email to ditelford.quality@draeger.com