Legal Notice
Our reference
-
Phone number
+49 451 882-6166
E-mail
matt.mckenna@draeger.com
Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory 2019-277-01

Infinity® M300 VG2.3.1 and earlier

This Product Security Advisory is based on facts known to us at the time of publication. However, there may be unknown or subsequent facts which may result in a revised assessment or may cause this assessment to be incorrect. As such, we reserve the right to change or revoke any recommendations at any time. In addition, this assessment does not take into account the specific facts that may exist in any given situation. Therefore, this assessment is provided “as-is” and without warranty and you assume sole responsibility for your actual use of the information. .

1 Publication Date

2019-10-09

2 Overview

At Dräger we develop technology for life which is why patient safety and medical device security are our top priorities. We endeavor to make our products as secure as possible against vulnerabilities that could affect the functioning of the products and the security, integrity and privacy of the electronic information and data used. We are committed to continuously improving the cyber security posture of our products and, as part of this effort and in line with our Coordinated Disclosure Policy, we are proactively issuing this advisory to make you aware of some potential cyber security risks with our Infinity M300 patient monitors (software version VG2.3.1 and earlier).

Dräger has identified that in the unlikely event that an unauthorized person who has the skills and the access to the hospital network could potentially cause the Infinity M300 device to reboot, lose alarm functionality, and/or lose communication with the Infinity Network.

Important Note: Draeger has received no reports of patient harm or successful exploits associated with these vulnerabilities.

3 How to verify if the product is affected

This advisory applies to Infinity M300 software version VG2.3.1 and earlier. To determine the software version for a specific Infinity M300 product:

a) Press menu button twice
b) Press the “down” arrow button 6 times
c) The software revision will now be displayed.

4 Vulnerability Description

The Infinity M300 patient worn monitor operates on the Hospital's wireless network infrastructure using a dedicated, isolated VLAN (subsequently referred to as the Infinity Network). During Dräger's internal penetration testing, the following vulnerabilities were identified:

If an unauthorized person launches a Denial of Service (DoS) attack on the hospital network, the Infinity network may be compromised which could lead to a reboot of the Infinity M300 and a loss of wireless network connectivity. A reboot takes approximately 30 seconds during which time there will a temporary loss of patient monitoring. Monitoring automatically resumes once the reboot completes. The Infinity CentralStation will audibly and visually alert staff that the affected Infinity M300 is offline.
The CVSSv3 Score for this vulnerability is 7.8.

In the unlikely event of an ongoing DoS attack causing a repeated reboot of the Infinity M300, the device would eventually enter a fail state requiring a manual restart of the Infinity M300. The CVSSv3 Score for this vulnerability is 8.3.

If the unauthorized person gains access to the Hospital network and is then able to breach the Infinity network, this could lead to a situation where data sent by the Infinity CentralStation to the Infinity M300 is compromised potentially allowing the attacker to change alarm settings, turn alarms off or put the Infinity M300 into Standby or Discharge. The CVSSv3 Score for this vulnerability is 4.8

Dräger has disclosed these potential vulnerabilities and mitigations to the relevant authorities and an advisory will be published via US-CERT (https://www.us-cert.gov/ics/advisories) and on the Dräger Product Security Website (https://static.draeger.com/security).

5 Remediation

To mitigate these cybersecurity concerns, Dräger will be releasing software version VG2.3.2 which is estimated to be available in March 2020.The upgrade path for your Infinity M300 device is dependent on the part number and your local Dräger representative will contact you prior to the release of the software patch to discuss the upgrade path.

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

6 Credit

Discovered through internal resources.

7 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 Dräger devices, please refer to https://static.draeger.com/security to contact the Product Security team directly.

8 Revision History

VERSION	DATE	COMMENTS
0.9	2019-10-09	Initial Draft Advisory

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:
Prof. Dr. Nikolaus Schweickart
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner