Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
-
Phone number
+01-978-379-6923

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 2019-331-01
SC Monitoring SC7000/SC9000

Legal Notice:

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

2019-11-21

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 a potential cyber security risks in the SC Monitoring SC7000/SC9000 patient monitors (all software versions).

Several vulnerabilities have been discovered in the Dräger SC7000/SC9000 Patient Monitoring Devices which can lead to information disclosure of device reboots of the patient monitors and privileged system access on the specified device.

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

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 all versions of the SC Monitoring product line: SC 6002XL, SC6802XL, SC 7000, SC8000, and SC90000 XL.

4 Vulnerability Description

The SC 6002XL, SC6802XL, SC 7000, SC8000, and SC90000 XL Dräger devices are affected by these vulnerabilities:

1. *Denial of Service (DoS)*
   A malformed network packet may cause the monitor to reboot.
2. *Hard-Coded Credentials*
   Plain-text credentials in source code.
   This vulnerability cannot be exploited remotely.

5 Impact

1. *Denial of Service:* By repeatedly sending the malformed network packet, an attacker is able to disrupt patient monitoring by causing the monitor to repeatedly reboot until it falls back to default configuration and loses network connectivity.
2. *Hard-Coded Credentials:* This vulnerability gives a local attacker access to the service and clinical account. Dräger has identified that in the unlikely event that an unauthorized person who has the skills and direct access to the SC7000/SC9000 patient monitor could potentially alter the device configuration. Altering the device configuration could lead to improper monitoring or reporting of the patient condition.

6 Severity

The CVSSv3 Scores for the vulnerabilities are:

1. *Denial of Service:* **Base** 6.5, **Temporal** 6.0
   CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C
2. Hard-Coded Credentials: **Base** 7.3, **Temporal** 7.3
   CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:H/RL:U/RC:C

7 Remediation

The SC Monitoring line, including SC 6002XL, SC6802XL, SC 7000, SC8000, and SC90000 XL, reached “End of Service” (EOS) effective December 31, 2011. As such there, this product is no longer maintained and there are no remediations.

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

8 Credit

This vulnerability was discovered by Jeroen Slobbe and Max Grim.

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

10 Revision History

VERSION	DATE	COMMENTS
0.9	2019-10-10	Initial
1.0	2019-11-22	Draft Advisory