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-20-064-1

SweynTooth Security Vulnerabilities

>> Dräger Medical Devices are not affected by SweynTooth 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.

To whom it may concern,

In February 2020 security researchers published vulnerabilities in implementations of the wireless technology Bluetooth Low Energy (BLE), named “SweynTooth”[1].
It is reported that the exploitation of these vulnerabilities can lead to device crashes, deadlocks and security bypasses[2]. So far, 12 vulnerabilities have been disclosed: CVE-2019-16336, CVE-2019-17060, CVE-2019-17061, CVE-2019-17517, CVE-2019-17518, CVE-2019-17519, CVE-2019-17520, CVE-2019-19192, CVE-2019-19193, CVE-2019-19194, CVE-2019-19195, and CVE-2019-19196.

[1] https://asset-group.github.io/disclosures/sweyntooth/
[2] https://www.fda.gov/medical-devices/safety-communications/sweyntooth-cybersecurity-vulnerabilities-may-affect-certain-medical-devices-fda-safety-communication

Impact

Dräger's Product Security team has received no reports of these vulnerabilities affecting clinical use of Dräger medical devices. Because Bluetooth Low Energy technology has not been deployed in Dräger medical devices, no such Dräger products are impacted by the aforementioned vulnerabilities.

Conclusion and Proposed Mitigations

For Dräger medical devices no action is necessary.

Further Information

If you have any further questions related to the impact of the SweynTooth vulnerabilities on Dräger medical devices, please contact your designated regional marketing manager. For reporting incidents and potential vulnerabilities in Dräger medical devices, please go to https://static.draeger.com/security to contact the Product Security team directly.

Best regards,

Dräger Product Security

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