Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
-
Phone number
+49 451 882-6166

E-mail
hannes.molsen@draeger.com
fabian.busch@draeger.com

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory 201902

Dräger ServiceConnect Client 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

2019-05-07

2 Overview

We have recently become aware of a security vulnerability in our Dräger ServiceConnect Client software which can lead to the disclosure of the Windows Logon Credentials to a local attacker if these are stored within the software settings as proxy server authentication credentials.

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 ServiceConnect Client, all software versions up to and including 3.7.0.144.

4 How to verify if the product is affected

Right click on the task icon , select `About…` and compare the displayed version number to the ones mentioned above. Furthermore, right click on the task icon, select `Settings` > `Proxy Settings…` and check whether username and password information is stored in the displayed fields of the dialog.

If you have a vulnerable software version AND stored proxy server credentials in the above described dialog you are affected.

5 Vulnerability Description

The proxy server credentials are stored unencrypted on the hard disk.

6 Impact

An attacker with access to the hard disk can read out the windows credentials of the affected user.

7 Severity

The CVSSv3 Scores for the vulnerability is:

Information Disclosure: **Base** 4.3 (Medium), **Temporal** 3.8
CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N/E:U/RL:T/RC:C

8 Remediation

A fixed version will be published to be downloaded and installed by customers by May 10. Customers should make sure to update the ServiceConnect Client software and afterwards verify as described in *4 How to verify if the product is affected* to have installed the correct and fixed version.

In the meantime, customers should consider removing the credentials from the above described `Proxy Settings…` dialog and confirm the deletion by clicking the `Save` button. It is furthermore recommended to change the affected credentials immediately, as they might have been read, dumped, or copied by an attacker.

9 Credit

The vulnerabilities were discovered and reported by an attentive customer. Thank you for helping us increasing the security and safety of our products!

10 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

11 Revision History

VERSION	DATE	COMMENTS
1.0	2019-05-07	Final 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:
Stefan Lauer
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner