

Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference

-

Phone number

+49 451 882-6166

Vulnerability and Incident Reporting

product-security@draeger.com

Dräger Product Security Advisory PSA-20-266-01

Security Vulnerabilities WIBU CodeMeter Runtime, used by Dräger Mobile Patient Watch, Dräger X-dock Manager, Dräger Polysoft, and Dräger REGARD Configuration Software.

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

2020-09-22

2 Overview

WIBU Systems disclosed vulnerabilities in CodeMeter Runtime, a product provided by WIBU Systems and used in some Dräger products for license management. Successful exploitation of these vulnerabilities could allow an attacker to alter and forge a license file, cause a denial-of-service condition, conduct remote code execution, or prevent normal operation of the software.

The full text of this advisory can be accessed through <https://static.draeger.com/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:
Stefan Lauer
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner

3 Affected Products

WIBU Systems CodeMeter Runtime up to version 7.10 is affected.

Installers of the following Dräger products integrate the vulnerable CodeMeter Runtime:

- Mobile Patient Watch, all versions up to 1.1.1
- X-dock Manager, all versions from 2.0 up to 3.0.2
- Dräger Polysoft, all versions up to 1.10.0
- REGARD Configuration Software, all versions from 01.00.00 up to 01.03.00

4 How to verify if the product is affected

- Find out the CodeMeter Runtime version:
 - o Find out where the codemeter.exe is located:
 - E.g. under: "C:\Program Files (x86)\CodeMeter\Runtime\bin\CodeMeter.exe"
 - Or open Services and check the properties of the "CodeMeter Runtime Server" service
 - o Open properties of codemeter.exe. The version is displays under "Details"

5 Vulnerability Description

CVE-2020-14509: CodeMeter Runtime DoS due to Buffer Access with Incorrect Length Value

This CVE vulnerability severity rating is 'Critical' (CVSS Rating: 10.0).

An attacker within the intranet where the Dräger product is deployed could send manipulated packets that can cause a crash of CodeMeter License Server or possibly inject and execute code.

CWE-805: Buffer Access with Incorrect Length Value

CVE-2020-14513: Improper Input Validation of Update Files in CodeMeter Runtime

This CVE vulnerability severity rating is 'High' (CVSS Rating: 7.5).

CodeMeter and the software using it may crash while processing a specifically crafted license file due to unverified length fields.

CWE-20: Improper Input Validation

CVE-2020-16233: CodeMeter Runtime API: Heap Leak

This CVE vulnerability severity rating is 'High' (CVSS Rating: 7.5).

An attacker could send a specially crafted packet that could have CodeMeter (All versions prior to 7.10) send back packets containing data from the heap.

CWE-404: Improper Resource Shutdown or Release

Other vulnerabilities from this disclosure (CVE-2020-14515, CVE-2020-14517) are without direct impact to the infrastructure of the customer, and have also been fixed by WIBU.

6 Impact

Mobile Patient Watch

The impact is negligible. The vulnerabilities are *not remotely exploitable*, as the CodeMeter Runtime in this installation is bound to localhost connections.

Other Products

An attacker could exploit the vulnerability remotely by sending a specially crafted message to the system node, causing the node to stop or become inaccessible, allowing the attacker to take control of the product or insert and run arbitrary code on the targeted machine.

7 Severity

See 5. for CVSS rating of the individual vulnerabilities.

8 Remediation

Mobile Patient Watch

- No action necessary. See 6.

Other Products

- Install version 7.10a of CodeMeter Runtime, downloadable from the WIBU website.

- Alternatively: For the Machine where the X-dock Manager Server is running, configure the firewall to block access to port TCP 22350 (If only Dräger products running on the machine use the CodeMeter Runtime)

Note:

- Mobile Patient Watch versions greater than 1.1.1 will include the fixed CodeMeter Runtime version.
- X-dock Manager versions from 3.0.3 will include the fixed CodeMeter Runtime version.
- REGARD Configuration Software versions greater than 01.03.00 will include the fixed CodeMeter Runtime version.
- Polysoft versions from 1.11.0 will include the fixed CodeMeter Runtime version.

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 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

10 Revision History

VERSION	DATE	COMMENTS
1	2020-09-22	Initial 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