Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-21-207-1

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-21-207-1

PrintNightmare Microsoft Windows Security Advisory

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

2021-07-26

2 Overview

From msrc.microsoft.com: “A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

At Dräger, your cybersecurity is our priority, which is why the product security team proactively analyzed all products that use Windows operating systems specifically for this vulnerability. The results confirmed that these products were either not exposed or can be protected by performing routine OS patching or following

the workarounds published by Microsoft. Dräger conducts testing on a monthly basis and confirms that our products are compatible with all patches. This will be checked on a monthly base and documented in a test report which the customer can get via https://www.draeger.com/de_de/Hospital/Hotfix or via the Dräger Service portal.

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

The following Dräger products are affected by this vulnerability:

- Integrated Care Manager (ICM)
  - Versions: 10.x, 11.x, 12.x, 13.x
- Innovian Anesthesia
  - Versions: 5.x, 6.x, 7.x, 8.x
- Infinity Explorer
  - Versions: 9.x, 10.x
- Infinity Gateway
  - Versions: 7.x, 9.x
- Mobile Patient Watch (MPW)
  - Versions: 1.x

4 How to verify if the product is affected

All product versions listed in Section 3 are affected.

5 Vulnerability Description

Remote Code Execution Vulnerabilities

CVE-2021-34527

CVE-2021-1675

6 Impact

An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

7 Severity

CVE-2021-34527

CVSS 3.1 Score

Base Score:	8.8
Severity:	High
Vector:	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

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

CVE-2021-1675
CVSS 3.1 Score

Base Score: 8.8
Severity: High
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

8 Remediation

Please visit msrc.microsoft.com for updated remediation instructions. Important details:

“In addition to installing the updates, in order to secure your system, you must confirm that certain registry settings are set to 0 (zero) or are not defined for the **Windows Server 2012, Windows Server 2016, and Windows 10, Version 1607 operating systems only** (Note: These registry keys do not exist by default, and therefore are already at the secure setting.), also that your Group Policy settings are correct.

Note that the security updates released on and after July 6, 2021 contain protections for CVE-2021-1675 and the additional remote code execution exploit in the Windows Print Spooler service known as ‘PrintNightmare’, documented in CVE-2021-34527.”

Specific Product Remediations

- Integrated Care Manager (ICM)
  - Operating system: Windows 7, Windows Server 2008 RC2
    - Affected registry keys exist: N/A
    - The Mainstream Support for Windows 7 and Windows Server 2008 RC2 is expired. ICM does not test and approve patches in the context of the monthly compatibility test. Draeger recommends following the recommendations shown in the Microsoft Remediation Advisory.
  - Operating system: Windows Server 2019
    - Affected registry keys exist: N/A
    - Specific remediation: apply latest Microsoft patches, see the Microsoft Remediation Advisory.

- Operating system: Windows Server 2012 RC2, Windows Server 2016 RC2, Windows 10
  - Affected registry keys exist: keys are not present by default
  - Specific remediation: apply latest Microsoft patches, see the Microsoft Remediation Advisory

- Innovian
  - Operating system: Windows 10 20H2
    - Affected registry keys exist: N/A
    - Specific remediation: apply latest Microsoft patches, see the Microsoft Remediation Advisory
  - Operating system: Windows Server 2016
    - Affected registry keys exist: keys are not present by default
    - Specific remediation: apply latest Microsoft patches, see the Microsoft Remediation Advisory
  - For all versions, additional recommendations:
    - For All CWS:
      - Set Computer Configuration \ Administrative Templates \ Printers \ “Allow Print Spooler to accept client connections” policy to “disabled” then restart the workstation or the Print Spooler Windows Service
    - For All Servers
      - Stop and disable the Print Spooler Windows Service

- Infinity Explorer
  - Operating system: Windows 7
    - Affected registry keys exist: N/A
    - Specific remediation: apply latest Microsoft patches, see the Microsoft Remediation Advisory

- Infinity Gateway
  - Operating system: Windows Server 2012 R2
    - Affected registry keys exist: keys are not present by default
    - Specific remediation: apply latest Microsoft patches, see the Microsoft Remediation Advisory
  - Operating system: Windows Server 2016
    - Affected registry keys exist: keys are not present by default
    - Specific remediation: apply latest Microsoft patches, see the Microsoft Remediation Advisory

- Mobile Patient Watch (MPW)
    - Operating system: Windows Server 2016
    - Affected registry keys exist: keys are not present by default
    - Specific remediation: apply latest Microsoft patches, see the Microsoft Remediation Advisory

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.

10 Revision History

VERSION	DATE	COMMENTS
1.0	2021-07-26	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