Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
-
Phone number
+49 451 882-6166

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 PSA-19-255-01

Microsoft Windows RDP RCE Security Advisory for CVE-2019-1181 and CVE-2019-1182

>> Dräger Medical Devices are not affected by CVE-2019-1181 and CVE-2019-1182.

>> Customer-Maintained Operating Systems can be patched according to the table in this document.

>> WARNING: Please note the special information for ICM!

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,

On August 13, 2019, Microsoft released information about a vulnerability in Microsoft Windows Remote Desktop Services / Terminal Services that allows remote attackers to execute arbitrary code via crafted packets. It is “wormable” and allows attackers to write exploits like WannaCry. The vulnerabilities CVE-2019-1181[1] and CVE-2019-1182[2] were published by Microsoft’s Security Response Center.

At Dräger, your cybersecurity is our priority, which is why the product security team proactively tested all products that use Windows operating systems specifically for this

[1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181
[2] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182

vulnerability. The results confirmed that these products were either not exposed or can be protected by performing routine OS patching.

Our medical devices running versions of Microsoft Windows without the two aforementioned patches remain secure due to the hardening of the operating systems. Our products run only the software and services needed for the operation of the device, therefore all embedded devices have RDP disabled, as it is not used. As a second line of defense, a software firewall independent from the operating system shields all network ports from traffic when they are not in use.

Product	Status
Infinity® Acute Care System (any version)	Not exposed: service disabled, port firewalled
Infinity® Explorer VF9/VF10 (Windows 7)	Update with the August rollup KB4512506
Infinity® Explorer older versions (Windows XP)	XP not affected by these vulnerabilities
Gateway/Symphony (Server 2008R2)	Update with the May rollup KB4499164
Gateway (old) (Server 2003)	Server 2003 not affected by these vulnerabilities
Innovian® Solution Suite	Update with the August rollup KB4512506
Innovian® Anesthesia (Windows 7)	Update with the August rollup KB4512506
Innovian® Anesthesia (Windows 10)	Update with the August rollup KB4512497

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

Zeus® Infinity® Empowered (Windows XP)	XP not affected by these vulnerabilities
SmartPilot® View 3.0n (Windows 7)	Update with the August rollup KB4512506
SmartPilot® View 2.0n (Windows XP)	XP not affected by these vulnerabilities
Evita® V300 (Windows XP)	XP not affected by these vulnerabilities
Evita® Infinity® V500 (Windows XP)	XP not affected by these vulnerabilities
Babylog® VN500 (Windows XP)	XP not affected by these vulnerabilities
PulmoVista® 500 (Windows XP)	XP not affected by these vulnerabilities
Integrated Care Manager (ICM) (Windows 2008 Server, Windows 7)	Update with the August rollup KB4512506 **and the additional KB4517297**[3]
Integrated Care Manager (ICM) (Windows 2012 Server)	Update with the August rollup KB4512488 **and the additional KB4517298**[4]
Integrated Care Manager (ICM) (Windows 2003 Server, Windows XP)	XP and 2003 Server not affected by these vulnerabilities

[3] The monthly rollup stopped VB6 code and thereby ICM from running. This was fixed with KB4517297 and therefore this is a **mandatory patch**!
[4] The monthly rollup stopped VB6 code and thereby ICM from running. This was fixed with KB4517298 and therefore this is a **mandatory patch**!

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

Further Information

- If an update with the aforementioned Microsoft hotfixes is not possible, customers should consider blocking TCP on port 3389 with an internal or external firewall to prevent access to the Remote Desktop Services. Microsoft further recommends to consider enabling Network Level Authentication (NLA). With NLA turned on, the attacker would first need to authenticate to Remote Desktop Services before being able to exploit the vulnerabilities.
- All other medical devices of Dräger are built or based on other embedded operating systems, which are not affected by this vulnerabilities. These devices include, but are not limited to: the Infinity® CentralStation, Infinity® M300, Infinity® M540, the Infinity Delta monitors, the Apollo®, Primus®, Fabius®, and Perseus® anesthesia devices, the Oxylog® emergency respirators, the Babylog® 8000 plus, Carina®, Evita® 2 dura, Evita® 4, Evita® XL, and Savina® ventilators, the Babyleo®, Caleo®, Isolette® thermoregulation devices.

Dräger routinely tests Microsoft operating system updates on products to verify there is no negative impact on overall software operation. For a copy of the monthly verified update report for Dräger monitoring, please contact your designated patient monitoring 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.

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:
Stefan Lauer
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner

Revisions

Version	Date	Change
1	2019-09-12	Initial Document

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