Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
-
Phone number
+49 451 882-6166

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

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory

WannaCry Ransomware

To whom it may concern,

On May 12, 2017, a global cyberattack infected hospitals, universities, manufacturers and government agencies in at least 150 countries.
The ransomware called “WannaCry” exploits a vulnerability in Microsoft Windows SMB Server that allows remote attackers to execute arbitrary code via crafted packets which essentially locks users out of their systems. The vulnerability was published as Microsoft Security Bulletin MS17-010[1] on March 14, 2017. Corporations that were not able to roll out the critical patches[2,3] can fall prey to this type of cyberattack and are charged hundreds of dollars to regain control of their data and documents.
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 vulnerability. The results confirmed that these products were either not exposed or could be protected by performing routine OS patching.

[1] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
[2] http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012218
[3] http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

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 most devices have SMB 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 March rollup KB4012218
Infinity® Explorer older versions (Windows XP)	Security update for XP KB4012598
Gateway/Symphony (Server 2008R2)	Update with the March rollup KB4012218
Gateway (old) (Server 2003)	Security update for XP KB4012598
Innovian® Solution Suite	Update with the March rollup KB4012218
Innovian® Anesthesia (Windows 7, Windows 10)	Update with the March rollup KB4012218
Infinity® C700 for IT (Windows 7)	Update with the March rollup KB4012218
Zeus® Infinity® Empowered (Windows XP)	Not exposed: service disabled, port firewalled

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

Zeus® (old) (Windows NT)	Not exposed: port firewalled
SmartPilot® View 3.0n (Windows 7)	Update with the March rollup KB4012218
SmartPilot® View 2.0n (Windows XP)	See Infinity® Explorer
Evita® V300 (Windows XP)	Not exposed: service disabled, port firewalled
Evita® Infinity® V500 (Windows XP)	Not exposed: service disabled, port firewalled
Babylog® VN500 (Windows XP)	Not exposed: service disabled, port firewalled
PulmoVista® 500 (Windows XP)	Not exposed: service disabled, port firewalled
Integrated Care Manager (ICM) (Windows 2008 Server, Windows 2012 Server, Windows 7, Windows 10)	Update with the March rollup KB4012218
Integrated Care Manager (ICM) (Windows 2003 Server, Windows XP)	Security update for XP KB4012598

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

Further Information

- If an update with Microsoft hotfixes is not possible, customers can block TCP port 445 with an internal or external firewall to prevent access to the server.
- KB4012598 (April rollup) is not yet fully verified for all devices, and is currently being evaluated
- The critical update was already included in the March rollup KB4012218 which should be installed.
- All other medical devices of Dräger are built or based on other embedded operating systems, which are not vulnerable to this attack. 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 systems or if you have any further questions related to the global ransomware attack, please contact your designated patient monitoring regional marketing manager. For reporting incidents and potential vulnerabilities in our devices, please refer to http://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

Additional Information on Ransomware

What is ransomware?
Ransomware is malicious software that locks a device, such as a computer, tablet or smartphone and then demand a ransom to unlock it.

Where did ransomware originate?
The first documented case appeared in 2005 in the United States, but quickly spread around the world.

How does it affect a computer?
The software is normally contained within an attachment to an email that masquerades as something innocent. Once opened it encrypts files on the hard drive, making it impossible to access or retrieve anything stored on there – such as photographs, documents, music, or important system files. Often not only files on the hard drive, but also files on connected network shares are being encrypted.

How can you protect yourself?
Users should always be very careful in opening attachments. Most ransomwares are spread as attachments to emails. Very often these are macro enabled Microsoft Office documents, where the user has to explicitly click to enable the malicious macro. Anti-virus software can – in most cases – only protect your machine against known viruses. Cybercriminals are constantly working on new ways to prevent detection of such protection mechanisms. Last but not least this attack has shown how important it is to keep your systems patched with the latest security updates.

How much are victims expected to pay?
The ransom demanded varies. However, there's no guarantee that paying will get your data back. For corporations the financial damage due to the required effort of the IT for cleaning or replacing the infected systems, and the resulting down time of the business exceed the damage of the encrypted files, as most businesses have working backup plans for lost data.

How is this ransomware attack different from the others?
This attack was a global coordinated ransomware attack. To infect systems, the attackers did not rely on phishing single users and infecting single systems by mail, but they exploited a Remote Code Execution vulnerability in Microsoft Windows. As thereby no user interaction was needed to run the malicious code, the infection spread as fast and broad as never before.

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

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

Revisions

Version	Date	Change
1	2017-05-15	Initial Document (EN)
2	2017-05-19	Translation: DE, IT, FR Additional tests: Zeus (old) Windows NT, Gateway Windows 2003 Removed footnotes after successful verification: ICM (KB4012598), Innovian Anesthesia (KB4012218) Renamed: Evita 2 -> Evita 2 dura

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