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 201703**

**Petya/Petna/NotPetya/PetrWrap Ransomware**

To whom it may concern,

On June 27, 2017, another global cyberattack infected computer systems worldwide. This ransomware is known, among others, under the names “Petya”, “Petna”, “NotPetya”, or “PetrWrap”. Like the WannaCry Ransomware attack in May it exploits the same 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. Additionally it spreads by issuing remote commands (PsExec) to machines on the local network (Windows Management Instrumentation Commandline - WMIC) while using credentials extracted from the infected machine. The huge difference to WannaCry is that this version of the malware only spreads via local networks, and not over the internet[4]. Systems patched according to our previous advisories 201701 and 201702 cannot be infected by exploiting MS17-010.

[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
[4] https://www.malwaretech.com/2017/06/petya-ransomware-attack-whats-known.html

Spreading via WMIC/PsExec remote commands can be exploited if an infected system contains cached access credentials that can be extracted using a tool called *mimikatz*[5]. A global “killswitch” like the one found for WannaCry is not known for the current ransomware, but there exists a “vaccine” that can be applied to every single computer system. It consists of a read-only file with the name *perfc.* If this file is present on the machine, different sources show that the current version of the Ransomware does not execute[6,7]. We advise our customers to consider distributing this file to prevent spreading of the Ransomware through local networks.

| 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<br>Consider distribution of the perfc file. |
| **Infinity® Explorer older versions** (Windows XP) | Security update for XP KB4012598<br>Consider distribution of the perfc file. |
| **Gateway/Symphony** (Server 2008R2) | Update with the March rollup KB4012218<br>Consider distribution of the perfc file. |
| **Innovian® Solution Suite** | Update with the March rollup KB4012218 |
| **Innovian® Anesthesia** (Windows 7, Windows 10) | Update with the March rollup KB4012218 |

[5] https://blog.kryptoslogic.com/malware/2017/06/28/petya.html
[6] https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak/
[7] https://eddwatton.wordpress.com/2017/06/27/use-group-policy-preferences-to-deploy-the-notpetya-vaccine/

| | |
|---|---|
| **Infinity® C700 for IT** (Windows 7) | Update with the March rollup KB4012218<br>Consider distribution of the perfc file. |
| **Zeus® Infinity® Empowered** (Windows XP) | Not exposed: service disabled, port firewalled |
| **SmartPilot® View 3.0n** (Windows 7) | Update with the March rollup KB4012218<br>Consider distribution of the perfc file. |
| **SmartPilot® View 2.0n** (Windows XP) | See Infinity® Explorer<br>Consider distribution of the perfc file. |
| **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<br>Consider distribution of the perfc file. |
| **Integrated Care Manager (ICM)** (Windows 2003 Server, Windows XP) | Security update for XP KB4012598<br>Consider distribution of the perfc file. |

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.
- 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, 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 ICM, or if you have any further questions related to the global ransomware attack, please contact your designated 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