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 201801

Meltdown and Spectre Vulnerabilities

To whom it may concern,

On January 3, 2018 security researchers have published vulnerabilities in multiple processor types which allow attackers to read out sensitive memory regions. The attacks exploit performance optimizations called “speculative execution” and “out of order execution”. It is possible to extract sensitive information like, e.g., passwords and private keys from protected kernel memory regions (“Meltdown Attack”[1], at the time of writing only Intel[2] and a minority of ARM[3] processors are vulnerable) or memory regions of different processes (“Spectre Attack”[4], at the time of writing works on AMD, ARM, and Intel[5]), which should normally be strictly separated. A protection mechanism against exploits called Address Space Layout Randomization in kernel space (“KASLR”) can also be circumvented by these attacks.
As these are vulnerabilities within the hardware chips, they can only be fully fixed by replacing the hardware. As this is in most cases infeasible, software vendors like Microsoft (KB4056892[6]) or the Linux project have started distributing mitigations that rely mostly on

[1] https://meltdownattack.com/meltdown.pdf
[2] https://newsroom.intel.com/press-kits/security-exploits-intel-products/
[3] https://developer.arm.com/support/security-update
[4] https://spectreattack.com/spectre.pdf
[5] https://newsroom.intel.com/news/intel-responds-to-security-research-findings
[6] https://www.theverge.com/2018/1/3/16846784/microsoft-processor-bug-windows-10-fix

switching off these performance optimizations. Thereby, strongly depending on the application scenario, worst case decreases in performance by up to 30% were observed. This affects mostly applications that rely heavily on Input/Output operations on disks and virtualized environments.
An attacker needs to be able to execute code under the attacker's control on the attacked machine.

Impact

Dräger embedded devices like ventilators, anesthesia devices, thermoregulation devices and patient monitors employ hardening mechanism that prevent the execution of any code not deployed with the device. This includes, e.g., a whitelisting of allowed processes, or the prevention of code execution from external storage devices, as well as development processes that minimize the risk of the appearance of remote code execution vulnerabilities due to, e.g., static code analysis, or code reviews. Considering these existing countermeasures for these devices the risk of patient safety issues due to the decreased performance after applying the previously mentioned software patches is way higher than the almost negligible risk of an actual cyberattack exploiting these vulnerabilities in such devices.

With Dräger products like the Infinity® C700 for IT Workstation customers are able to install and run, e.g., clinical software applications of different manufacturers. Before applying the Microsoft patch (KB4056892) it is crucial to verify whether a possible performance decrease caused by the patch is acceptable.

Patches for the underlying operating systems or third party software on which Dräger software applications like ICM or Dräger Monitoring Systems are running, are routinely verified. We are currently in the process of verifying our software systems against the respective patches. Customers are able to receive a copy of the monthly verified update report by contacting their designated regional marketing manager.

Conclusion and Proposed Mitigations

For Dräger embedded devices no action is necessary.

For Infintiy® C700 for IT apply KB4056892, but it is crucial to verify the system performance.

For Dräger software solutions please wait for the next monthly verified update reports before applying KB4056892.

Further Information

If you have any further questions related to the impact of the Meltdown or Spectre attacks on Dräger devices, 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.

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