Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
-
Phone number
+49 451 882-6166

E-mail
hannes.molsen@draeger.com
detlef.koeble@draeger.com

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-20-216-1

CVE-2020-1350 "SIGRed" (Windows DNS Server Remote Code Execution Vulnerability)

>> Dräger Medical Devices are not affected by "SIGRed"

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 July 14, 2020, the security company CHECKPOINT Research released information about a critical vulnerability in the Windows DNS Servers (CVE-2020-1350) that could allow remote code execution when they fail to properly handle DNS responses. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the Local System Account. Windows servers that are configured as DNS servers are at risk from this vulnerability.

Dräger Medical Devices do not include Windows DNS Server as a component. Therefore they are not affected by the vulnerability.

Patches for the underlying operating systems on which Dräger software applications like ICM and Infinity Gateway 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.

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

Revisions

VERSION	DATE	CHANGE
1.0	2020-08-03	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