Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-22-193-1

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-22-193-1

CVE-2022-30190 (Follina)

>> Dräger Medical Products (Devices and Software) are not affected by CVE-2022-30190

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.

1 Publication Date

2022-07-12

2 Overview

On May 30, 2022, Microsoft has released an advisory[1] regarding a remote code execution vulnerability in the Microsoft Support Diagnostic Tool (MSDT) called Follina. The Cybersecurity & Infrastructure Agency (CISA) published an alert[2] about Follina on May 31, 2022. On Tuesday June 14, 2022, Microsoft issued a patch as

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

[2] https://www.cisa.gov/uscert/ncas/current-activity/2022/05/31/microsoft-releases-workaround-guidance-msdt-follina-vulnerability

part of their monthly Windows update to address this vulnerability. Microsoft recommends installing the updates as soon as possible.

The vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. The attacker can then install programs, view, change, or delete data, or create new accounts in the context allowed by the user's rights.

None of Dräger medical products are affected by CVE-2022-30190 (Follina). Dräger software-only products based on the MS Windows operating system are compatible to the patch provided as part of the monthly Windows update.

This advisory will be updated if there are new findings about this vulnerability that affect Dräger Medical Products.

The full text of this advisory can be accessed through https://static.draeger.com/security.

Revision History

VERSION	DATE	COMMENTS
1.0	2022-07-12	Initial Advisory

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