Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-22-63-1

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-22-63-1

CVE-2021-4034 PwnKit Advisory

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

2022-03-04

2 Overview

On January 25, 2022, Qualys disclosed a memory corruption vulnerability (CVE-2021-4034) found in polkit's pkexec utility. This vulnerability can easily be exploited for local privilege escalation. Polkit is a component for controlling system-wide privileges in Unix-like operating systems.

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

3 Affected Products

The following Dräger products are affected by this vulnerability:

- Infinity Central Station (ICS) VG2.1.2 and VG3

4 How to verify if the product is affected

Hover the mouse pointer over the Draeger logo on the lower right side of the display to see the version of the ICS.

5 Vulnerability Description

Out-of-bounds Write (CWE-787)
CVE-2021-4034

A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code.

6 Impact

When successfully executed the attack can cause a local privilege escalation giving unprivileged users administrative rights on the target machine.

7 Severity

CVSS 3.1

Base Score:	7.8
Severity:	High
Vector:	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

8 Remediation

ICS VG2 versions are based on CentOS6. A patch for this version is provided starting with the February 2022 patches for CentOS6.
ICS VG3 versions are based on CentOS7. A patch for this version is provided starting with the February 2022 patches for CentOS7.

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

These patches are now available on Service Connect to be downloaded and installed by approved service personnel.

The vulnerability will be completely removed with the provided patches.

9 Contact Information

If you have any further questions related to the impact of the vulnerabilities, 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.

10 Revision History

VERSION	DATE	COMMENTS
1.0	2022-03-04	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