Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-22-154-1

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-22-154-1

Dräger Clinical Assistance Package (CAP 1.0) Security Vulnerability

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

2022-06-03

2 Overview

A security vulnerability was identified in the OpenSSL library used by CAP 1.0 devices. The vulnerability could allow a remote attacker to carry out a denial of service attack on the device.

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

3 Affected Products

The following Dräger products part of the CAP 1.0 are affected by this vulnerability:

- Dräger CC300 Version 1.1.2 and 1.1.3
- Dräger IACS VG7.1/VG7.1.1
- Infinity Gateway VF9.0/VF9.0.1

4 How to verify if the product is affected

To verify the version of software on the Dräger IACS and Infinity Gateway devices: Open the information screen on the devices to review the software version. The software version is also displayed on the screen during device startup.

5 Vulnerability Description

Loop with Unreachable Exit Condition ('Infinite Loop') (CWE-835)

CVE-2022-0778

From National Vulnerability Database:

“The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters.”

6 Impact

- Dräger CC300 Version 1.1.2 and 1.1.3: An attack could cause a reboot of the device.
- Dräger IACS VG7.1/VG7.1.1: SDC devices may not be accessible and secondary alarm data from the SDC devices on the network may be lost.
- Infinity Gateway VF9.0/VF9.0.1: SDC devices may not be accessible and secondary alarm data from the SDC devices on the network may be lost.

7 Severity

National Vulnerability Database CVSS 3.1 Score

Base Score:	7.5
Severity:	High
Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

8 Remediation

The remediations differ per device:

- Dräger CC300 Version 1.1.2 and 1.1.3: The vulnerability will not result in an unacceptable risk to health for patients, users or bystanders. No user action is required. In the course of a future product bugfix this vulnerability may be fixed.
- Dräger IACS VG7.1/VG7.1.1 A risk assessment has been performed and the risk has been deemed acceptable. There is no remediation available.
- Infinity Gateway VF9.0/VF9.0.1: A risk assessment has been performed and the risk has been deemed acceptable. Infinity Gateway can be configured to receive all the data from Infinity devices except for some secondary alarm data from SDC. The Gateway applications will continue to function successfully. For VF9.1, SDC functionality will be removed, thereby remediating the threat.

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	2022-06-03	Initial Advisory