Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
-
Phone number
+49 451 882-6166

E-mail
hannes.molsen@draeger.com
fabian.busch@draeger.com

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory 201901

Infinity® Delta Family Security Vulnerabilities

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

2019-01-22

2 Overview

Several vulnerabilities have been discovered in the Dräger Infinity® Delta Family of Patient Monitoring Devices which can lead to information disclosure of device logs, denial of service through device reboots of the patient monitors, and privilege escalation on the connected Infinity® C700-for-IT cockpit with running Infinity® Explorer.

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

3 Affected Products

The following Dräger devices are affected by these vulnerabilities:

- Dräger Infinity® Delta, Delta XL, Kappa, all software versions.
- Dräger Infinity® Explorer C700, all software versions

4 How to verify if the product is affected

All software versions of the previously specified products are affected. The vulnerabilities 3 and 4 (see 5 Vulnerability Description) affecting the Infinity® Explorer C700 have already been fixed in earlier software versions, but as this is a system release, in order to use Infinity® Explorer C700 together with patched Infinity® Delta, Delta XL, or Kappa VF10.1 Patient Monitors customers need to update the Infinity® Explorer C700 to VF10.1 as well (see 8 Remediation).

5 Vulnerability Description

5.1 Vulnerabilities affecting the Infinity® Delta, Delta XL, and Kappa Patient Monitors

1. *Denial of Service*
   A malformed network packet may cause the monitor to reboot.
2. *Information Disclosure*
   Log files are accessible over an unauthenticated network connection.

5.2 Vulnerabilities affecting the Infinity® Explorer C700

3. *Elevation of Privilege*
   Via a specific dialog it is possible to break out of the kiosk mode and reach the underlying operating system.
4. *Outdated Software*
   Several 3rd party components were found outdated and vulnerable to several published security vulnerabilities.

6 Impact

1. By repeatedly sending the malformed network packet, an attacker is able to disrupt patient monitoring by causing the monitor to repeatedly reboot until it falls back to default configuration and loses network connectivity.
2. By accessing the log files an attacker is able to gain insights about internals of the patient monitor, the location of the monitor, and wired network configuration.
3. By breaking out of the kiosk mode an attacker is able to take control of the operating system and thereby, e.g., cause the Infinity® Explorer to display wrong or no information from the connected Delta Family patient monitor.
4. By using vulnerabilities in the outdated components an attacker would be able to launch further attacks on the system, and thereby, e.g., cause the Infinity® Explorer to display wrong or no information from the connected Delta Family patient monitor.

7 Severity

The CVSSv3 Scores for the vulnerabilities are:

1. *Denial of Service:* **Base** 6.5, **Temporal** 6.0
   CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C
2. *Information Disclosure:* **Base** 4.3, **Temporal** 4.0
   CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C
3. *Privilege Escalation:* **Base** 8.4, **Temporal** 7.8
   CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
4. *Outdated Software:* Several vulnerabilities known to affect the latest version of Windows XP SP3

8 Remediation

All Vulnerabilities have been fixed in the Delta / Infinity® Explorer VF10.1 software releases of the affected components. The software is available through Dräger Service as of December 2018. The fix contains the following improvements:

1. *Denial of Service:* The Delta VF10.1 software drops malformed network packages, thus preventing the device from rebooting.
2. *Information Disclosure:* The affected ports have been closed in the Delta VF10.1 software.
3. *Privilege Escalation:* The Infinity® Explorer VF10.1 software does prevent leaving the kiosk mode.
4. *Outdated Software:* The Infinity® Explorer VF10.1 software runs on Windows 7. Dräger regularly releases a list of tested and approved operating system patches, so that customers can regularly update their systems.

9 Credit

The vulnerabilities were discovered and reported by Marc Ruef and Rocco Gagliardi, scip AG. Thank you for helping us increasing the security and safety of our products!

10 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.

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

11 Revision History

VERSION	DATE	COMMENTS
0.9	2018-12-21	Initial Draft Advisory
1.0	2019-01-22	Final Advisory, Coordinated Disclosure with NCCIC

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