Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-25-076-1

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-25-076-1

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

2025-03-17

2. Overview

On January 30, 2025, the FDA issued a safety communication highlighting cybersecurity vulnerabilities in the Contec CMS8000 and Epsimed MN-120 patient monitors [2]. On the same day, CISA released a fact sheet detailing a backdoor vulnerability in the Contec CMS8000 firmware. Testing revealed that the affected firmware version can mount a remote NFS share from an IP address that is not registered to the device manufacturer but is instead associated with a university [1]. This configuration may allow unauthorized remote access, posing potential risks to device integrity and patient data security.

3. Dräger Products

In collaboration with our manufacturing partner, we have conducted a review of our Dräger Vista monitoring portfolio, which includes:

Vista 120 V3/S
Vista 120 SC
Vista 300
Vista 120 CMS
Vista CMS

Our evaluation involved both internal assessments and third-party penetration testing designed to simulate potential attack vectors similar to those identified in the Contec CMS8000. We can confirm that none of the Dräger Vista monitors exhibit the backdoor vulnerability. Detailed testing of the Vista 120 patient monitor, among others, revealed no evidence of unauthorized remote access points.

Dräger Medical Products remains steadfast in its commitment to cybersecurity excellence. We continuously monitor the threat landscape and work closely with regulatory and cybersecurity agencies to ensure our products are secure. Although our devices are not affected by the identified backdoor vulnerability, we will update this advisory immediately should new findings emerge regarding any potential impact on Dräger Medical products.

4. Contact Information

For further questions regarding the vulnerabilities or their impact, please contact your designated regional marketing manager. To report incidents or potential vulnerabilities in our devices, visit our Product Security website at https://static.draeger.com/security and reach out directly to our Product Security team.

5. References

[1] CISA Fact Sheet: Contec CMS8000 Contains Backdoor
[2] FDA Safety Communication: Cybersecurity Vulnerabilities in Certain Patient Monitors

Use of this document / contents is forbidden without express authority. All rights reserved. Refer to protection notice ISO 16016.
Printed copies are uncontrolled and for reference purposes only.

6. Change log

Version	Date	Change notes
1.0	2025-03-17	Initial Advisory

Use of this document / contents is forbidden without express authority. All rights reserved. Refer to protection notice ISO 16016.
Printed copies are uncontrolled and for reference purposes only.