Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-26-174-1

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-26-174-1

Windows Secure Boot certificate expiration in Dräger Infinity® Acute Care System (IACS) / Infinity® Central Station (ICS) / Medical Grade PCs (ACL)

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

2026-06-23

2. Overview

Three Microsoft UEFI Secure Boot certificates issued in 2011 expire in 2026, two of them in June 2026. Dräger Infinity® Acute Care System (IACS) SW VG8.0 and VG9.0 as well as ACL Medical Grade PCs run Windows with Secure Boot enabled and are affected. Infinity® Central Station (ICS) VG 6 on Gen 5 Hardware runs Red Hat Enterprise Linux, which uses a Microsoft-signed UEFI shim loader for Secure Boot and is therefore also affected. For all investigated Dräger products, the certificate expiration does not cause operational failures: devices will continue to start and operate normally after the expiration dates. The impact is a gradual reduction in the ability to receive certain Secure Boot-related security updates, specifically updates to Windows Boot Manager, Secure Boot databases, revocation lists, and protections against newly identified boot-level vulnerabilities.

3. Affected Products

- Dräger Infinity® Acute Care System (IACS) SW VG8.0 and VG9.0
- Dräger Infinity® Central Station (ICS) VG 6 - Gen 5 Hardware (MS41214)
- ACL Medical Grade PCs where Secure Boot is enabled in BIOS

4. How to verify if the product is affected

Infinity® Acute Care System (IACS): Go to Menu > System Setup > Biomed > Service to verify the software version.

Infinity® Central Station (ICS): Identify the hardware generation by part number. Gen 5 Hardware (MS41214) has Secure Boot enabled and is affected. Gen 4 Hardware (MS32504) does not support Secure Boot and is not affected.

ACL Medical Grade PCs: Check whether Secure Boot is active in the BIOS. Devices shipped by ACL with Secure Boot disabled (the default at delivery) are not affected. Only devices where Secure Boot was activated after delivery require the BIOS update.

5. Vulnerability Description

Microsoft's UEFI Secure Boot infrastructure relies on X.509 certificates stored in device firmware to validate bootloaders at startup. Three certificates issued by Microsoft in 2011 are reaching end of validity in 2026:

- **Microsoft Corporation KEK CA 2011** - expires 2026-06-24. Used to authenticate updates to the Secure Boot Signature Database (DB/DBX).
- **Microsoft Corporation UEFI CA 2011** - expires 2026-06-27. Authenticates third-party UEFI bootloaders and option ROMs.
- **Microsoft Windows Production PCA 2011** - expires 2026-10-19. Authenticates Windows Boot Managers signed before the 2023 transition.

Microsoft has issued replacement certificates (2023 series).

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. Impact

Affected devices with Secure Boot enabled and outdated firmware certificates will no longer be able to receive certain security updates related to the early boot process, if they are signed with the 2023 replacement certificates.

Devices continue to start and operate normally; there is no immediate risk of operational failure for the investigated Dräger products.

7. Severity

N/A - Not a CVE-based advisory.

8. Remediation

Infinity® Acute Care System (IACS) SW VG8.0 and VG9.0: A new BIOS containing the 2023 replacement certificates will be shipped in one of the upcoming software releases.

Infinity® Central Station (ICS) VG 6 - Gen 5 Hardware (MS41214): Remediation is under investigation. Dräger will provide further information as soon as it becomes available.

ACL Medical Grade PCs: BIOS update packages containing both the 2011 and 2023 certificates are available from ACL for units where Secure Boot is enabled. As ACL PCs were delivered with Secure Boot disabled by default, no immediate action is required for standard field units. Customers who have Secure Boot enabled can download the applicable BIOS update packages directly from the ACL customer login area (www.acl.de/de/loginbereich). Packages are device-specific - submit a serial number list to the ACL dealer to receive the correct packages per unit. For certain devices under part number MS90100 Dräger will also publish the updates via MyDräger.

9. Credit

N/A

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.

11. Change log

Change notes
2026-06-23: Initial release

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.