Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-26-175-1

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-26-175-1

Dräger Infinity CentralStation 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.

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.

1. Publication Date

2026-06-24

2. Overview

Recently, multiple high-profile Linux kernel vulnerabilities have been disclosed by various security researchers. Several of these vulnerabilities are considered "universal" Linux vulnerabilities, meaning they potentially impact a broad range of Linux distributions and kernel versions.

The Infinity Central Station product family uses different Linux versions depending on the platform and software release. The purpose of this advisory is to clarify the current status, applicability, and remediation plans related to these vulnerabilities for the affected product versions.

This advisory currently covers the following vulnerabilities (a more detailed technical description is provided in Section 5):

- CopyFail - CVE-2026-31431
- DirtyFrag - CVE-2026-43284 and CVE-2026-43500
- Fragnesia - CVE-2026-46300
- ssh-keysign-pwn - CVE-2026-46333
- Pack2theRoot - CVE-2026-41651
- DirtyCBC - CVE-2026-31635

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

3. Affected Products

The following software versions of Infinity CentralStation are impacted:

Vulnerability	CVE	VG6.0	VG4.0/5.0
2026-06-24: Initial release	CVE-2026-31431	Affected	Not affected [1]
DirtyFrag	CVE-2026-43284	Affected	Not affected [1]
DirtyFrag	CVE-2026-43500	Not affected [2]	Not affected [2]
Fragnesia	CVE-2026-46300	Affected	Not affected [1]
ssh-keysign-pwn	CVE-2026-46333	Affected	Not affected [3]
Pack2theRoot	CVE-2026-41651	Affected	Not affected [4]
DirtyCBC	CVE-2026-31635	Not affected [2]	Not affected [2]

[1] CentOS 7 kernel (3.10) predates the vulnerable code path; Red Hat confirms only RHEL 8+ affected

[2] Affected module/codepath not present in any CentralStation configuration

[3] Exploitation requires pidfd_getfd(2) syscall (kernel 5.6+), not available on kernel 3.10

[4] PackageKit package not installed on Infinity CentralStation VG4.0/5.0

4. How to verify if the product is affected

Enter the console and run the following command to verify the kernel has been updated:

```
rpm -q kernel --last | head -1
```

If the displayed kernel version is 4.18.0-553.124.1.el8_10 or later and the install date is on or after 2026-06-01, the cumulative hotfixes have been applied.

If you are unsure whether your installed version meets this requirement, contact your Dräger service representative.

5. Vulnerability Description

CopyFail - CVE-2026-31431:

CWE-1288: Improper Validation of Consistency within Input

A flaw was found in the Linux kernel's algif_aead cryptographic algorithm interface. An incorrect in-place operation causes source and destination data mappings to differ during cryptographic processing. A low-privileged local attacker can exploit this flaw to corrupt the contents of sensitive system files and escalate to root privileges.

DirtyFrag - CVE-2026-43284 and CVE-2026-43500:

CWE-123: Write-what-where Condition

CVE-2026-43284 - A flaw was found in the Linux kernel's xfrm-ESP and RxRPC subsystems. Unsafe in-place cryptographic processing of shared socket buffer fragments allows a low-privileged local attacker to corrupt page-cache contents of readable files, including sensitive system files, and gain root privileges. The xfrm-ESP variant requires unprivileged user or network namespace creation, while the RxRPC variant depends on the rxrpc module being available on the target system.

CVE-2026-43500 - A flaw was found in the Linux kernel's RxRPC networking subsystem. When a socket buffer carrying a page-cache reference reaches the RxRPC authentication verification path, the kernel performs an in-place decryption directly on the referenced page without first isolating the buffer. A low-privileged local attacker can exploit this behavior to corrupt the page-cache contents of readable files, including sensitive system files such as /etc/passwd, and obtain root privileges. Exploitation does not require unprivileged user or network namespaces, but depends on the RxRPC protocol stack being available on the target system.

Fragnesia - CVE-2026-46300:

CWE-123: Write-what-where Condition

A flaw was found in the Linux kernel's XFRM ESP-in-TCP subsystem. Unsafe in-place cryptographic processing allows a low-privileged local attacker to write arbitrary bytes into the page cache of read-only files, including sensitive system files. An attacker can exploit this to overwrite privileged binaries and gain root privileges.

ssh-keysign-pwn - CVE-2026-46333:

CWE-269: Improper Privilege Management

A vulnerability was found in the Linux kernel that allows an unprivileged local user to read sensitive files normally restricted to the root user. The flaw occurs during process exit, where a brief window allows an attacker to intercept file access from a privileged process before it fully terminates. Successful exploitation may lead to the disclosure of sensitive data such as SSH host private keys or /etc/shadow contents.

Pack2theRoot - CVE-2026-41651:

CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

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.

A flaw was found in PackageKit. A time-of-check time-of-use (TOCTOU) race condition on transaction flags allows unprivileged users to install packages as root, resulting in a local privilege escalation.

DirtyCBC - CVE-2026-31635:

CWE-130: Improper Handling of Length Parameter Inconsistency

A flaw was found in the Linux kernel's rxrpc component. An inverted length check in the rxgk_verify_response() function allows oversized RESPONSE authenticators to be accepted. This can lead to an impossible length being passed to skb_to_sgvec(), triggering a BUG_ON condition and resulting in a system crash, effectively causing a Denial of Service (DoS).

6. Impact

The system command line is not accessible to standard users during normal operation. Both the local GUI console and remote SSH access require elevated credentials (sms_user account password), which must be configured before the system can be used for patient monitoring.

Successful exploitation would allow an attacker to escalate privileges to root (CVE-2026-31431, CVE-2026-43284, CVE-2026-46300, CVE-2026-41651) or read sensitive system files including password hashes and SSH host keys (CVE-2026-46333). With root access, an attacker could modify system configuration, access patient data, or disrupt monitoring availability.

These vulnerabilities do not enable remote exploitation over the network and cannot be triggered without first authenticating to the system command line.

7. Severity

CVSS Score: 8.8

Severity: High

Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

8. Remediation

Infinity CentralStation VG6.0:

The May 2026 hotfixes for Infinity CentralStation VG6.0 include fixes for the following issues:

- CopyFail - CVE-2026-31431
- DirtyFrag - CVE-2026-43284
- Pack2theRoot - CVE-2026-41651

Please apply the hotfixes to remediate these issues. These hotfixes are cumulative; applying the latest hotfix includes all previous security fixes.

The June 2026 hotfixes will have fixes for the following issues:

- Fragnesia - CVE-2026-46300
- ssh-keysign-pwn - CVE-2026-46333

Infinity CentralStation VG4.0/5.0:

Infinity CentralStation VG4.0 and VG5.0 are based on CentOS 7. Based on current analysis, including kernel version review, package inventory, and proof-of-concept testing, Dräger has assessed Infinity CentralStation VG4.0 and VG5.0 are not impacted.

Dräger recommends upgrading to Infinity CentralStation VG6.0 where available, in order to benefit from faster and more comprehensive security updates for the underlying operating system and system packages.

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.

Hotfixes can be found on Dräger ServiceConnect®. Please contact your Dräger service representative for assistance locating and installing hotfixes.

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
New Attachment for Product Security 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.