CISA Flags Critical Flaws in J4Care dcm4chee-arc-light 5.35.1



CISA published an advisory on J4Care dcm4chee-arc-light 5.35.1, rated CVSS v3 9.1. Flaws could let attackers delete medical images, expose patient data, inject forged studies or cause denial of service.

- Affected: dcm4chee-arc-light 5.35.1 from J4Care, a company headquartered in Austria.
- Six CVEs are listed, including CVE-2026-97851, with a CVSS v3 score of 9.1.
- Weakness types: missing authorization, missing authentication for a critical function, infinite loop and inefficient algorithmic complexity.
- Possible impact: deletion of stored images, patient data disclosure, forged studies, reassigned patient records, overwritten files and denial of service.
- CVE-2026-97851: the storage status-change REST service can mark locations for deletion, causing

> stored objects to be purged while database records remain.

CISA has published an ICS medical advisory covering J4Care dcm4chee-arc-light version 5.35.1. The product is used in healthcare and public health, and the advisory lists a CVSS v3 score of 9.1.

What the advisory describes

Six CVEs are listed: CVE-2026-97851, CVE-2026-107621, CVE-2026-105273, CVE-2026-101021, CVE-2026-105279 and CVE-2026-105667. The weakness types include **missing authorization**, **missing authentication for a critical function**, an infinite loop and inefficient algorithmic complexity.

According to CISA, successful exploitation could let an attacker delete stored medical images, disclose patient information, inject forged studies, reassign patient records, overwrite files and cause a denial-of-service condition.

One example is CVE-2026-97851. The storage status-change REST service allows location records tied to DICOM instances to be switched to deletion-related states. If a location is set to TO_DELETE, the PurgeStorageScheduler deletes the referenced object from storage, even though the instance record stays in the database.

What to do

The excerpt does not describe a vendor fix or workaround, so teams should check the full CISA advisory and J4Care channels for remediation guidance. Healthcare institutions running this archive should confirm whether version 5.35.1 is deployed, review who can reach its REST services, and check the integrity of imaging stores and patient-record linkage. Because patient data and imaging availability are involved, treat this as a clinical-safety and privacy matter as well as a security one.

What to do now

1. Inventory systems to find any dcm4chee-arc-light 5.35.1 deployments.
2. Read the full CISA advisory and contact J4Care for patches or mitigations.
3. Restrict network access to the archive's REST services to trusted systems and users only.
4. Verify integrity of stored images and patient-record associations, and confirm backups are intact and restorable.
5. Review access and application logs for unexpected storage status changes or deletions.
6. Assess PDPL notification duties if unauthorized disclosure of patient data is suspected.