CISA تحذّر من ثغرات حرجة في J4Care dcm4chee-arc-light الإصدار 5.35.1



نشرت CISA تنبيهاً بشأن J4Care dcm4chee-arc-light 5.35.1 بدرجة CVSS v3 تبلغ 9.1، وقد تتيح الثغرات حذف الصور الطبية أو كشف بيانات المرضى أو حقن دراسات مزوّرة أو تعطيل الخدمة.

- المتأثر: dcm4chee-arc-light الإصدار 5.35.1 من J4Care، وهي شركة يقع مقرها في النمسا.
- أُدرجت ست ثغرات (CVE) منها CVE-2026-97851، بدرجة CVSS v3 تبلغ 9.1.
- أنواع الضعف: غياب التفويض، وغياب المصادقة لوظيفة حرجة، وحلقة لا نهائية، وتعقيد خوارزمي غير فعّال.
- الأثر المحتمل: حذف الصور المخزنة، وكشف بيانات المرضى، وحقن دراسات مزوّرة، وإعادة إسناد سجلات المرضى، وإتلاف الملفات، وتعطيل الخدمة.
- CVE-2026-97851: خدمة REST لتغيير حالة التخزين قد تضع مواقع الملفات في حالة حذف، فتُزال الكائنات المخزنة بينما تبقى سجلات قاعدة البيانات.

نشرت CISA تنبيهاً طبياً يخص أنظمة التحكم الصناعي حول J4Care dcm4chee-arc-light الإصدار 5.35.1. يُستخدم المنتج في قطاع الرعاية الصحية والصحة العامة، ويذكر التنبيه درجة CVSS v3 تبلغ 9.1.

ما الذي يصفه التنبيه

أُدرجت ست ثغرات هي: CVE-2026-97851 وCVE-2026-107621 وCVE-2026-105273 وCVE-2026-101021 وCVE-2026-105279 وCVE-2026-105667. وتشمل أنواع الضعف **غياب التفويض** و**غياب المصادقة لوظيفة حرجة** وحلقة لا نهائية وتعقيداً خوارزمياً غير فعّال.

وبحسب CISA قد يتمكن المهاجم عند الاستغلال الناجح من حذف الصور الطبية المخزنة، وكشف معلومات المرضى، وحقن دراسات مزوّرة، وإعادة إسناد سجلات المرضى، وإتلاف الملفات، وتعطيل الخدمة.

من الأمثلة CVE-2026-97851: تتيح خدمة REST الخاصة بتغيير حالة التخزين تحويل سجلات المواقع المرتبطة بنسخ DICOM إلى حالات متصلة بالحذف. وعند ضبط الموقع على TO_DELETE يحذف PurgeStorageScheduler الكائن المشار إليه من التخزين، بينما يبقى سجل النسخة في قاعدة البيانات.

ما العمل

لا يذكر المقتطف إصلاحاً من المورّد أو حلًا بديلًا، لذا ينبغي مراجعة تنبيه CISA الكامل وقنوات J4Care للحصول على إرشادات المعالجة. وعلى المنشآت الصحية التي تشغّل هذا الأرشيف التأكد من نشر الإصدار 5.35.1، ومراجعة من يستطيع الوصول إلى خدمات REST، والتحقق من سلامة مخازن الصور وارتباط سجلات المرضى. ولأن الأمر يمس بيانات المرضى وتوافر الصور، فهو شأن يتعلق بسلامة المرضى والخصوصية إضافة إلى الأمن.

ما يجب فعله الآن

1. حصر الأنظمة لتحديد أي نشر لـ dcm4chee-arc-light الإصدار 5.35.1.
2. قراءة تنبيه CISA كاملًا والتواصل مع J4Care للحصول على التحديثات أو التدابير المخففة.
3. حصر الوصول الشبكي إلى خدمات REST في الأرشيف على الأنظمة والمستخدمين الموثوقين فقط.
4. التحقق من سلامة الصور المخزنة وارتباط سجلات المرضى، والتأكد من سلامة النسخ الاحتياطية وقابليتها للاستعادة.
5. مراجعة سجلات الوصول والتطبيق بحثاً عن تغييرات أو عمليات حذف غير متوقعة في حالة التخزين.
6. تقييم التزامات الإبلاغ وفق نظام حماية البيانات الشخصية (PDPL) عند الاشتباه في كشف غير مصرح به لبيانات المرضى.