ثغرة في Baicells Nova 430H eNodeB قد تتسبب في انقطاع مؤقت للخدمة (CVE-2026-96274)



أفادت CISA بأن أجهزة Baicells Nova 430H eNodeB حتى الإصدار BaiBLQ_3.0.12 قد تتعطل برسالة مشوهة من جهاز قريب غير موثّق. تقييم CVSS v3 هو 7.4.

- الأجهزة المتأثرة: Nova 430H eNodeB (الطراز pBS3101SH) بالإصدارات حتى BaiBLQ_3.0.12 ضمنًا.
- الثغرة CVE-2026-96274 من نوع استثناء غير معالج، بتقييم CVSS v3 قدره 7.4.
- يمكن لجهاز غير موثّق ضمن نطاق الإرسال الراديوي إرسال رسالة مشوهة تحتوي حمولة NAS غير صالحة أثناء إعداد الاتصال.
- لا تتحقق المحطة من الحمولة وتمررها إلى الشبكة الأساسية، مما قد يوقف ارتباط الإشارات الخاص بالخلية.
- الأثر انقطاع مؤقت للخدمة حتى يعيد eNodeB والشبكة الأساسية الاتصال.

نشرت CISA نشرة استشارية ضمن أنظمة التحكم الصناعي بشأن Baicells Nova 430H، وهو جهاز eNodeB يُستخدم في شبكات الاتصالات الخلوية. يندرج المنتج ضمن قطاعي الاتصالات وتقنية المعلومات، وينتشر عالميًا، ويقع المقر الرئيسي للشركة المصنّعة في الولايات المتحدة.

طبيعة الثغرة

تحمل الثغرة المعرّف **CVE-2026-96274** وتقييم CVSS v3 قدره 7.4. وتشمل جهاز Nova 430H eNodeB من الطراز pBS3101SH بالإصدارات حتى BaiBLQ_3.0.12 ضمنًا.

أثناء إعداد الاتصال، يستطيع جهاز غير موثّق ضمن نطاق الإرسال الراديوي إرسال رسالة صاعدة مشوهة تحتوي حمولة NAS غير صالحة. لا يتحقق eNodeB من هذه الحمولة بالشكل الصحيح ويمررها إلى الشبكة الأساسية، وقد يؤدي ذلك إلى إيقاف ارتباط الإشارات الخاص بالخلية.

الأثر

النتيجة حجب خدمة مؤقت، إذ تنقطع الخدمة في الخلية إلى أن يعيد eNodeB والشبكة الأساسية إنشاء الاتصال. ولا تشير المصدر إلى سرقة بيانات أو تنفيذ تعليمات برمجية.

الخطوات المقترحة

على الجهات التي تشغّل بنية خلوية خاصة أو مُدارة، أو تعتمد عليها، التأكد أولاً من استخدام هذا الطراز ومن إصدار البرنامج الثابت. ولا يذكر المقتطف المتاح إصدارًا مصححًا أو إجراءً تخفيفيًا من الشركة، لذا يُنصح بمراجعة نشرة CISA الكاملة وإرشادات Baicells قبل التخطيط لأي تغيير.

ما يجب فعله الآن

1. مراجعة سجل الأصول للتحقق من وجود أجهزة Baicells Nova 430H eNodeB من الطراز pBS3101SH وتوثيق إصدارات البرنامج الثابت.
2. اعتبار الإصدارات حتى BaiBLQ_3.0.12 ضمنًا متأثرة وإدراجها ضمن أولويات متابعة الثغرات.
3. الاطلاع على نشرة CISA الكاملة والتواصل مع Baicells أو مزوّد التكامل للحصول على الإصلاحات أو إجراءات التخفيف.
4. التأكد مع مشغّل الاتصالات أو مزوّد التكامل من أثر انقطاع الخلية على الخدمات الحرجة ومراجعة ترتيبات البدائل.
5. رصد حالات إيقاف ارتباط الإشارات المتكررة أو إعادة تشغيل الخلايا غير المبررة وتصعيدها عبر مسار معالجة الحوادث.