# CISA تحذّر من ثغرات حرجة في تطبيق EseeCloud وبرنامجه الثابت لكاميرات IP



نشرت CISA تنبيهًا لأنظمة التحكم الصناعي عن ثلاث ثغرات في تطبيق EseeCloud وبرنامجه الثابت قد تتيح للمهاجم السيطرة على كاميرات IP. درجة CVSS v3 هي 9.8.

- المتأثر: تطبيق EseeCloud حتى الإصدار 4.9.6 والبرنامج الثابت حتى 4.9.86.0.
- ثلاث ثغرات: CVE-2026-107617 وCVE-2026-97858 وCVE-2026-105664.
- أنواع الضعف: بيانات اعتماد مضمّنة في الشيفرة، وتعديل غير مضبوط لخصائص الكائنات، واختلاف في الاستجابة يمكن رصده.
- إحدى الثغرات تتيح الدخول إلى الأجهزة ببيانات اعتماد مضمّنة.
- لم تردّ الشركة المصنّعة Guangzhou Juan IoT Technology على محاولات التنسيق من CISA.

أصدرت CISA تنبيهًا يخص أنظمة التحكم الصناعي بشأن منتجات EseeCloud من شركة Guangzhou Juan IoT Technology. ويفيد التنبيه بأن استغلال الثغرات الثلاث قد يمنح المهاجم سيطرة على كاميرات IP المتأثرة، وبدرجة CVSS v3 قدرها 9.8.

## المنتجات المتأثرة

يشمل التنبيه إصدارات تطبيق EseeCloud حتى 4.9.6 وما دونها، والبرنامج الثابت EseeCloud حتى 4.9.86.0 وما دونه. وتنطبق الثغرات الثلاث على كليهما: CVE-2026-107617 وCVE-2026-97858 وCVE-2026-105664.

أنواع الضعف هي: استخدام بيانات اعتماد مضمّنة في الشيفرة، وتعديل غير مضبوط لخصائص الكائنات المحددة ديناميكيًا، واختلاف في الاستجابة يمكن رصده. وفي الثغرة CVE-2026-107617 يستطيع المهاجم استخدام بيانات اعتماد مضمّنة لتسجيل الدخول إلى أجهزة EseeCloud.

## موقف الشركة والسياق

تذكر CISA أن الشركة المصنّعة لم تردّ على محاولات التنسيق. والمقتطف الذي راجعناه لا يذكر إصلاحًا من الشركة، لذا ينبغي التخطيط لضوابط تعويضية بدل انتظار تحديث.

وتذكر CISA أن القطاعات المعنية هي الطاقة والاتصالات وأنظمة النقل والخدمات المالية والخدمات والمرافق الحكومية، مع انتشار عالمي، وأن مقر الشركة في الصين.

## ما العمل

ابدؤوا بحصر أي كاميرات تعتمد على EseeCloud، بما في ذلك الفروع والمرافق والمواقع التي يديرها طرف ثالث، ثم قلّلوا تعرّضها للشبكة ما دام موقف الشركة غير واضح.

## ما يجب فعله الآن

1. حصر جميع كاميرات IP والتطبيقات التي تستخدم EseeCloud، بما فيها ما يديره طرف ثالث.
2. التحقق من وجود الإصدارات المتأثرة (التطبيق حتى 4.9.6 والبرنامج الثابت حتى 4.9.86.0).
3. إزالة هذه الكاميرات من التعرّض المباشر للإنترنت وعزلها في شبكة مجزّأة.
4. حصر الوصول إلى واجهات إدارة الكاميرات بالمسؤولين المصرّح لهم فقط.
5. رصد أي عمليات دخول أو تغييرات إعدادات غير متوقعة على هذه الأجهزة.
6. الاستفسار من الموردين عن موقف الشركة من المعالجة، والنظر في استبدال الأجهزة إذا لم يتوفر إصلاح.