

تنبيه حول ثغرة برمجيات كاميرات VIVOTEK



توجد ثغرة في برمجيات كاميرات VIVOTEK قد تسمح بتنفيذ أوامر عن بُعد، مما يعرض نظام الكاميرا للخطر. يجب على المؤسسات التي تستخدم النماذج المتأثرة اتخاذ إجراءات فورية لتقليل المخاطر.

- توجد ثغرة في برمجيات كاميرات VIVOTEK تسمح بتنفيذ أوامر عن بُعد.
- النماذج المتأثرة تشمل مجموعة من كاميرات السلسلة V و C.
- يمكن أن يؤدي الاستغلال الناجح إلى تعريض نظام الكاميرا للخطر بالكامل.
- يوصى باتخاذ إجراءات فورية للمؤسسات التي تستخدم هذه الأجهزة.

نظرة عامة

أبلغت VIVOTEK عن ثغرة حرجية في برمجيات كاميراتها قد تمكن المهاجمين من تنفيذ أوامر عن بُعد، مما قد يؤدي إلى الحصول على صلاحيات الجذر وتعريض نظام الكاميرا للخطر بالكامل. تؤثر هذه الثغرة على عدة نماذج من السلسلتين V و C.

النماذج المتأثرة

تؤثر الثغرة على النماذج التالية من كاميرات VIVOTEK: السلسلة V FD9187، FD9189، FD9365، FD9387، FD9389، FD9391، FE9180، FE9191، FE9382، FE9391، IB9365، IB9387، IB9389، IB939، IP9165، IP9171، IP9172، IP9181، IP9191، IT9389، MA9321، MA9322، MS9321، وغيرها. يجب على المؤسسات التي تستخدم هذه النماذج تقييم تعرضها.

الإجراءات الموصى بها

لتقليل المخاطر المرتبطة بهذه الثغرة، يجب على المؤسسات اتخاذ الإجراءات التالية:

- مراجعة قائمة نماذج كاميرات VIVOTEK المتأثرة المستخدمة.
- تحديث برمجيات الأجهزة المتأثرة إلى أحدث إصدار تقدمه VIVOTEK.
- تنفيذ تقسيم الشبكة للحد من الوصول إلى أنظمة الكاميرات.
- مراقبة حركة الشبكة لرصد أي نشاط غير عادي يتعلق بأجهزة الكاميرات.
- إجراء تدقيق أمني على أنظمة الكاميرات لتحديد الثغرات المحتملة.

ما يجب فعله الآن

1. مراجعة قائمة نماذج كاميرات VIVOTEK المتأثرة المستخدمة.
2. تحديث برمجيات الأجهزة المتأثرة إلى أحدث إصدار تقدمه VIVOTEK.
3. تنفيذ تقسيم الشبكة للحد من الوصول إلى أنظمة الكاميرات.
4. مراقبة حركة الشبكة لرصد أي نشاط غير عادي يتعلق بأجهزة الكاميرات.
5. إجراء تدقيق أمني على أنظمة الكاميرات لتحديد الثغرات المحتملة.