

إشعار بشأن ثغرة Hitachi Energy SOI



حددت شركة Hitachi Energy ثغرة **تنفيذ الشيفرة عن بُعد** في مكون Apache ActiveMQ لمنتج SOI الخاص بها. يجب على المؤسسات التي تستخدم الإصدارات المتأثرة اتخاذ إجراءات فورية للتخفيف من المخاطر.

- تؤثر الثغرة على إصدارات SOI بين 2.0.0 و 2.2.0.
- قد يؤدي الاستغلال إلى المساس بالسرية والنزاهة وتوافر المنتج.
- يوصى باتخاذ إجراءات فورية للتخفيف من المخاطر المحتملة.

نظرة عامة

أبلغت شركة Hitachi Energy عن ثغرة تنفيذ الشيفرة عن بُعد في مكون Apache ActiveMQ لمنتج SOI الخاص بها. تؤثر هذه المشكلة على إصدارات معينة من منتج SOI، مما يسمح للمهاجمين المحتملين باستغلال الثغرة، مما قد يؤدي إلى مخاطر أمنية كبيرة.

التأثير

يمكن أن تؤثر الثغرة على **السرية والنزاهة وتوافر** منتج SOI. يجب على المؤسسات التي تستخدم الإصدارات المتأثرة أن تكون على دراية بالعواقب المحتملة وأن تتخذ الاحتياطات اللازمة لحماية أنظمتها.

الإجراءات الموصى بها

لتخفيف المخاطر المرتبطة بهذه الثغرة، يجب على المنظمات اتخاذ الخطوات التالية:

- مراجعة الإصدار الحالي من منتج SOI المستخدم.
- الترقية إلى إصدار غير متأثر من SOI في أقرب وقت ممكن.
- تنفيذ تدابير أمنية لتقييد الوصول إلى مكون Apache ActiveMQ.
- مراقبة الأنظمة لأي نشاط غير عادي قد يشير إلى محاولات استغلال.
- البقاء على اطلاع على التحديثات والإشعارات من شركة Hitachi Energy بشأن هذه الثغرة.

ما يجب فعله الآن

1. مراجعة الإصدار الحالي من منتج SOI المستخدم.
2. الترقية إلى إصدار غير متأثر من SOI في أقرب وقت ممكن.
3. تنفيذ تدابير أمنية لتقييد الوصول إلى مكون Apache ActiveMQ.
4. مراقبة الأنظمة لأي نشاط غير عادي قد يشير إلى محاولات استغلال.
5. البقاء على اطلاع على التحديثات والإشعارات من شركة Hitachi Energy بشأن هذه الثغرة.