Ivanti تصدر تحديثات لثغرتين إضافيتين من نوع يوم الصفر في Connect Secure استُغلّتا معًا



أصدرت Ivanti تحديثات لثغرتين إضافيتين في بوابات الوصول عن بُعد Connect Secure (ICS)، استُغلّتا معًا في هجمات يوم الصفر منذ 1 أكتوبر على الأقل.

- أصلحت Ivanti ثغرتين إضافيتين في Connect Secure (ICS)، وهو بوابة الوصول عن بُعد التابعة لها.
- جرى استغلال الثغرتين معًا في هجمات يوم الصفر، أي قبل توفر الإصلاح.
- يحدد المصدر بداية الهجمات في 1 أكتوبر على الأقل.
- لا يتضمن المقتطف المتاح أرقام CVE أو الإصدارات المتأثرة أو تفاصيل الضحايا.

نشرت Ivanti تحديثات أمنية لثغرتين إضافيتين في Connect Secure (ICS)، وهو بوابة الوصول عن بُعد التابعة لها. ووفقًا لموقع BleepingComputer، استُغلّت الثغرتان معًا في هجمات يوم الصفر الجارية منذ 1 أكتوبر على الأقل.

ما المعروف حتى الآن

جرى استغلال الثغرتين بصورة متسلسلة، وبدأ الاستغلال قبل توفر الإصلاحات. ويصف التقرير الثغرتين بأنهما إضافيتان إلى مشكلات سابقة في Connect Secure. ولا يذكر المقتطف المتاح لنا أرقام CVE ولا نطاقات الإصدارات المتأثرة ولا طبيعة نشاط المهاجمين، لذا ينبغي الرجوع إلى نشرة Ivanti الرسمية لهذه التفاصيل.

أهمية الموضوع

تقع بوابات الوصول عن بُعد على حافة الشبكة ويمكن الوصول إليها من الإنترنت، ما يجعلها هدفًا متكررًا. وبما أن الاستغلال يعود بحسب التقرير إلى 1 أكتوبر على الأقل، فعلى الجهات التي تشغّل ICS افتراض أن الجهاز ربما تعرّض للخطر قبل تثبيت التحديث، وألا تكتفي بالتحديث وحده.

النهج المقترح

تأكدوا من وجود ICS في بيئتكم، بما يشمل الشركات التابعة ومزوّدي الخدمة من الأطراف الثالثة. وطبّقوا تحديثات المورّد سريعًا ضمن إجراءات التغيير الطارئ، وراجعوا الجهاز بحثًا عن مؤشرات اختراق تغطي الفترة منذ بداية أكتوبر. واتبعوا إرشادات Ivanti لأي فحوصات سلامة توصي بها.

ما يجب فعله الآن

1. حصر جميع أجهزة ICS) Connect Secure)، بما فيها التي تديرها الشركات التابعة أو أطراف ثالثة.
2. تطبيق أحدث تحديثات Ivanti ضمن إجراء التغيير الطارئ.
3. مراجعة السجلات وتنفيذ فحوصات السلامة التي توصي بها Ivanti بحثًا عن مؤشرات اختراق منذ بداية أكتوبر.
4. تغيير بيانات الاعتماد والأسرار التي يتعامل معها الجهاز عند الاشتباه بالاختراق.
5. الإبلاغ عن الحوادث المؤكدة عبر قنوات الجهة التنظيمية، مثل الهيئة الوطنية للأمن السيبراني أو البنك المركزي السعودي حسب الاختصاص.