تحذير من FBI وCISA بشأن هجمات سيبرانية تستهدف أنظمة التبريد



حذّرت FBI وCISA من هجمات سيبرانية تستهدف أنظمة التبريد. تعذّرت قراءة نص المصدر، لذا لا نعرض تفاصيل، وننصح بالرجوع إلى التحذير الأصلي.

- حذّرت FBI وCISA معًا من هجمات سيبرانية تستهدف أنظمة التبريد.
- كان نص المصدر الذي وصلنا تالفًا، لذلك لا نذكر هنا التفاصيل التقنية أو المنتجات المتأثرة أو الجداول الزمنية.
- أنظمة التبريد جزء من التقنيات التشغيلية التي تعتمد عليها جهات الغذاء والدواء والخدمات اللوجستية.
- يُنصح بمراجعة تقرير BleepingComputer الأصلي وتحذير الجهتين مباشرة.

ما الذي ورد في التقرير

أفاد موقع BleepingComputer بأن FBI وCISA حذّرتا من هجمات سيبرانية تستهدف أنظمة التبريد. غير أن النص الذي وصلنا لإعداد هذا الخبر كان غير مقروء، ولذلك لا يمكننا بمسؤولية وصف أساليب الهجوم أو الموردين المتأثرين أو الضحايا أو إجراءات التخفيف الموصى بها.

لماذا يهم ذلك

أصبحت معدات سلسلة التبريد متصلة بالشبكات بصورة متزايدة، وغالبًا ما تُدار خارج برنامج الأمن السيبراني الأساسي لتقنية المعلومات. وقد تعتمد عليها جهات الغذاء والرعاية الصحية والأدوية والخدمات اللوجستية في استمرارية أعمالها، لذا يستحق تحذير صادر عن جهتين وطنيتين مراجعة داخلية سريعة حتى قبل الاطلاع على كامل التفاصيل.

الخطوات المقترحة

اطلعوا على التقرير الأصلي وتحذير الجهتين، ثم تحققوا مع فرق المرافق والعمليات مما إذا كانت أنظمة التبريد أو إدارة المباني متصلة بأي شبكة، ومن يتولى صيانتها، وكيف تُراقب. وطبّقوا الإرشادات الفنية الواردة في التحذير بعد التحقق منها، دون الاعتماد على هذا الملخص وحده.

ما يجب فعله الآن

1. اقرأوا تقرير BleepingComputer الأصلي وتحذير FBI وCISA كاملاً.
2. احصروا أنظمة التبريد وإدارة المباني وحدّدوا المتصل منها بالشبكات.
3. تأكدوا مع فرق المرافق ومقدمي الصيانة من الأطراف التي لديها وصول عن بُعد إلى هذه الأنظمة.
4. تحققوا من شمول هذه الأنظمة بالمراقبة وخطط الاستجابة للحوادث.
5. طبّقوا إجراءات التخفيف الفنية الواردة في التحذير بعد التحقق من ملاءمتها لبيئتكم.