Synology تحث على تحديث DSM بعد هجمات فدية استهدفت أجهزة NAS



أفادت Synology برصد هجمات فدية على أجهزة NAS التي تعمل بإصدارات قديمة من DSM، عبر ثغرة صُححت في ديسمبر 2024، وطالبت العملاء بالتحديث.

- تفيد Synology بأن مهاجمين يستغلون ثغرة في نظام DSM (DiskStation Manager).
- صُححت الثغرة في ديسمبر 2024، والأجهزة المستهدفة هي التي تعمل بإصدارات DSM قديمة.
- تقول الشركة إن الهجمات تهدف إلى تشفير البيانات وطلب فدية.
- تحث Synology العملاء على تحديث DSM.

دعت Synology، الشركة التايوانية المصنّعة لأجهزة التخزين المتصل بالشبكة (NAS)، عملاءها إلى تحديث نظام DSM (DiskStation Manager) الذي يشغّل أجهزتها، بعد رصدها هجمات فدية.

ما أعلنته الشركة

تذكر الشركة أن جهات التهديد تستغل ثغرة سبق أن صححتها في ديسمبر 2024، وأن الهجمات تستهدف الأجهزة التي ما زالت تعمل بإصدارات قديمة من DSM. وأوضحت في بيانها أن غاية هذه الهجمات تشفير البيانات وابتزاز الضحايا للحصول على فدية.

لا يتضمن المصدر تفاصيل فنية إضافية، كرقم CVE أو عدد الأجهزة المتأثرة أو هوية المهاجمين، ولذلك لا نتكهن بها هنا.

أهمية الخبر

يذكّرنا الحدث بأن إصلاحاً صدر منذ فترة لا يحمي إلا الأنظمة التي طُبّق عليها. وغالباً ما تحتوي أجهزة NAS على مجلدات مشتركة ونسخ احتياطية، فقد يؤثر هجوم فدية عليها في العمليات وفي خيارات الاستعادة معاً.

الإجراءات المقترحة

على الجهات التي تستخدم أجهزة Synology NAS تحديد إصدارات DSM المثبتة لديها وتحديثها وفق إرشادات الشركة، ومراجعة نشرة الشركة الأمنية بحثاً عن أي تعليمات خاصة بطرازاتها.

ما يجب فعله الآن

1. حصر جميع أجهزة Synology NAS وتوثيق إصدارات DSM عليها.
2. تحديث أي جهاز يعمل بإصدار DSM قديم وفق إرشادات Synology.
3. مراجعة نشرة الشركة الأمنية للاطلاع على تعليمات خاصة بكل طراز.
4. التأكد من سلامة النسخ الاحتياطية الموجودة على أجهزة NAS أو قربها وإمكانية استعادتها.
5. توثيق معالجة هذه الأجهزة ضمن عملية إدارة الثغرات.