برنامج Thermo Fisher Torrent Suite: ثغرة اجتياز مسار تتيح قراءة ملفات على الخادم



أفادت CISA بوجود ثغرة اجتياز مسار (CVE-2026-107777) في Torrent Suite Software حتى الإصدار 5.18، تتيح لمهاجم موثّق قراءة ملفات على Torrent Server. توصي Thermo Fisher بالتحديث إلى 5.22 أو أحدث.

- الإصدارات المتأثرة: Torrent Suite Software حتى الإصدار 5.18.
- الثغرة CVE-2026-107777 من نوع اجتياز المسار (CWE-22) بدرجة CVSS v3 تبلغ 6.5.
- يمكن لمهاجم موثّق قراءة ملفات عشوائية على Torrent Server يستطيع حساب خدمة الويب الوصول إليها.
- أصلحت Thermo Fisher المشكلة في الإصدار 5.22 وما بعده.
- تصنّف CISA القطاع المعني بالرعاية الصحية والصحة العامة، مع انتشار المنتج عالمياً.

نشرت CISA نشرة استشارية طبية بشأن برنامج Thermo Fisher Torrent Suite Software تتناول ثغرة اجتياز مسار تحمل الرمز CVE-2026-107777.

المنتجات المتأثرة

تؤثر الثغرة في الإصدار 5.18 وما قبله من Torrent Suite Software، وسببها عدم تقييد مسارات الملفات بالشكل الصحيح ضمن المجلد المسموح (CWE-22). تبلغ درجة CVSS v3 ما مقداره 6.5. وتصنّف CISA القطاع المعني بالرعاية الصحية والصحة العامة، مع انتشار المنتج حول العالم.

الأثر

يمكن لمهاجم سبق أن حصل على مصادقة قراءة ملفات عشوائية على Torrent Server، ويقتصر ذلك على الملفات التي يمكن لحساب خدمة الويب الوصول إليها. ولا تشير النشرة إلى استغلال فعلي للثغرة.

الإصلاح والخطوات التالية

أصلحت Thermo Fisher الثغرة وتوصي بالتحديث إلى Torrent Suite Software الإصدار 5.22 أو أحدث، وتتوفر تفاصيل إضافية في نشرتها الأمنية.

على الجهات التي تشغّل هذا البرنامج، مثل المختبرات والمنشآت الصحية والبحثية، التحقق من إصدارها وجدولة التحديث ومراجعة الحسابات الممنوحة على الخادم. وبما أن الاستغلال يتطلب مصادقة، فإن ضبط الحسابات يقلل التعرض إلى حين تنفيذ التحديث.

ما يجب فعله الآن

1. حصر أي نسخ من Torrent Suite Software وتسجيل إصداراتها.
2. تحديث النسخ ذات الإصدار 5.18 أو أقدم إلى 5.22 أو أحدث.
3. مراجعة النشرة الأمنية لدى Thermo Fisher للاطلاع على إرشادات التخفيف الإضافية.
4. مراجعة الحسابات التي يمكنها المصادقة على Torrent Server وتقليصها.
5. التحقق من الملفات التي يصل إليها حساب خدمة الويب وتقليل الصلاحيات غير الضرورية.