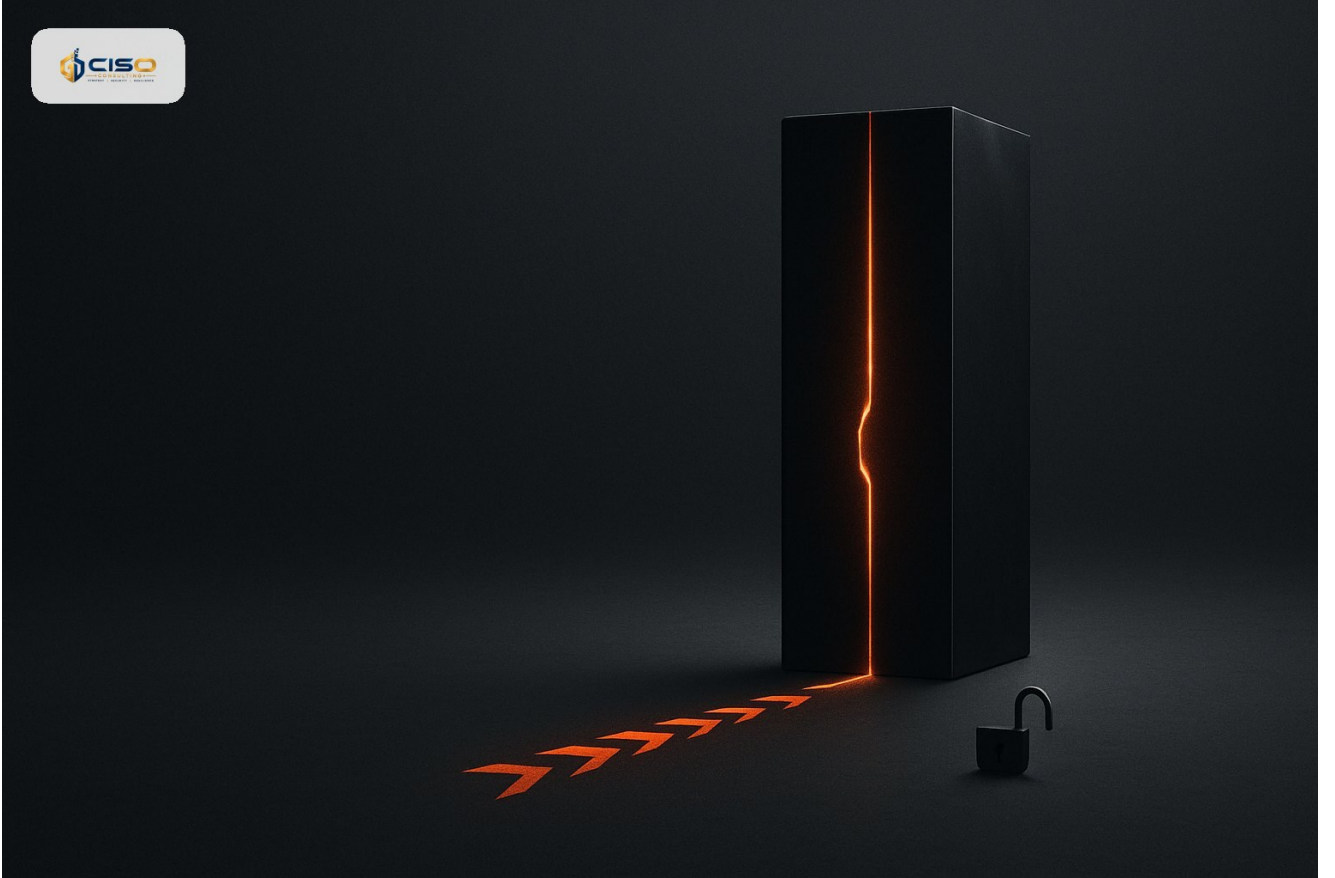


إصدار استغلال علني لثغرة FortiSIEM الحرجة CVE-2026-106173



صدر استغلال تجريبي علني للثغرة (CVE-2026-106173) (CVSS 9.4) في Fortinet FortiSIEM، وهي ثغرة اجتياز مسار مُعالجة تتيح لمهاجم غير مصادق تنفيذ تعليمات أو أوامر غير مصرح بها.

- نشر باحثون استغلالاً تجريبياً لثغرة في FortiSIEM جرى إصلاحها حديثاً.
- الثغرة مسجلة برقم CVE-2026-106173 وبتقييم CVSS قدره 9.4 (حرجة).
- هي ثغرة اجتياز مسار يمكن أن يستغلها مهاجم غير مصادق لتنفيذ تعليمات أو أوامر غير مصرح بها.
- وجود استغلال علني يجعل الأنظمة غير المحدثة أسهل استهدافاً.

نشر باحثون استغلالاً تجريبياً (PoC) لثغرة حرجة في Fortinet FortiSIEM سبق أن أصدرت الشركة إصلاحاً لها. الثغرة مسجلة برقم CVE-2026-106173 وتبلغ درجتها 9.4 وفق مقياس CVSS.

ما هو معروف

تتعلق المشكلة بضعف اجتياز المسار (path traversal). وبحسب التقرير، يمكن لمهاجم غير مصادق استغلالها لتنفيذ تعليمات أو أوامر غير مصرح بها على النظام المتأثر. ولا يتطلب ذلك بيانات اعتماد، وهذا سبب التصنيف الحرج. لا يذكر المقتطف المتاح الإصدارات المتأثرة أو الإصدارات المعالجة، ولا يؤكد وقوع استغلال فعلي. ينبغي الرجوع إلى نشرة Fortinet الرسمية لهذه التفاصيل.

أهمية الأمر

كثيراً ما يكون FortiSIEM في صميم المراقبة الأمنية إذ يجمع السجلات من مختلف أرجاء البيئة. وقد يؤثر اختراق منصة كهذه في مستوى الرؤية وفي الثقة بالبيانات التي تحتفظ بها. وعندما يصبح الاستغلال التجريبي متاحاً للعموم، تميل المدة بين صدور الإصلاح ومحاولات الاستغلال إلى الانكماش، لذا ينبغي للجهات التي لم تطبق الإصلاح بعد أن تعدّه أولوية.

الخطوات التالية

تحقق من وجود FortiSIEM في بيئتك، وقارن الإصدار بنشرة Fortinet، وجدول تطبيق الإصلاح عبر مسار التغيير الطارئ. وإلى حين ذلك، قيّد الوصول الشبكي إلى واجهات المنصة بحيث يقتصر على شبكات الإدارة الموثوقة.

ما يجب فعله الآن

1. حصر جميع نسخ FortiSIEM بما فيها بيانات الاختبار والتعافي من الكوارث.
2. مقارنة الإصدارات المثبتة بنشرة Fortinet الخاصة بـ CVE-2026-106173 وتطبيق الإصلاح عبر إدارة التغيير الطارئ.
3. حصر الوصول إلى واجهات FortiSIEM في شبكات الإدارة الموثوقة إلى حين التحديث.
4. مراجعة سجلات FortiSIEM والشبكة بحثاً عن طلبات غير معتادة أو أوامر غير متوقعة منذ صدور الإصلاح.
5. توثيق التعرض والمعالجة في سجل إدارة الثغرات والمخاطر لأغراض المراجعة من الجهات التنظيمية.