# Siemens RUGGEDCOM APE1808: ثغرة double free في FortiOS من Fortinet (CVE-2026-106175)



تنقل CISA إشعار Siemens بشأن أجهزة RUGGEDCOM APE1808 العاملة ببرنامج Fortinet NGFW والمتأثرة بثغرة double free في FortiOS. توصي Siemens بالتحديث إلى الإصدار V7.6.9 أو أحدث.

- جميع إصدارات RUGGEDCOM APE1808 مع Fortinet NGFW مدرجة ضمن المنتجات المتأثرة.
- الثغرة CVE-2026-106175 من نوع (CWE-415 (Double Free في FortiOS وFortiProxy وFortiSwitch.
- يمكن لمهاجم محلي مصادَق عليه أن يتسبب في تعطل خدمة newcli عبر أوامر CLI مُعدّة خصيصاً.
- درجة CVSS v3 المذكورة هي 2.3، أي منخفضة.
- توصي Siemens بتحديث Fortigate NGFW إلى V7.6.9 أو أحدث وفق إجراء التحديث الآمن.

## ما الذي نُشر

أعادت CISA نشر إشعار من Siemens يخص RUGGEDCOM APE1808، وهو منتج صناعي يمكن أن يعمل ببرنامج جدار الحماية من الجيل التالي من Fortinet. ويأتي الإشعار بعد إعلان Fortinet عن ثغرة Double Free برقم (CWE-415) (CVE-2026-106175 في FortiOS وFortiProxy وFortiSwitch.

## الأثر

وفق المصدر، يستطيع مهاجم محلي سبق أن صودق عليه استخدام أوامر CLI مُعدّة خصيصاً لإيقاف خدمة newcli عن العمل. وتبلغ درجة CVSS v3 المذكورة 2.3، أي أن الخطورة منخفضة. وتُصنَّف جميع إصدارات RUGGEDCOM APE1808 مع Fortinet NGFW ضمن المنتجات المتأثرة. ومقر Siemens في ألمانيا، ويذكر الإشعار قطاع التصنيع الحيوي والانتشار حول العالم.

## المعالجة الموصى بها

توصي Siemens بتحديث Fortigate NGFW إلى الإصدار V7.6.9 أو أحدث باتباع إجراء التحديث الآمن لديها، مع إمكانية الحصول على التفاصيل عبر دعم العملاء.

نظراً لانخفاض الدرجة واشتراط الوصول المحلي المصادَق عليه، فالمطلوب معالجة ضمن دورة التحديث المعتادة لا إجراء طارئاً. ومع ذلك ينبغي للجهات التي تشغّل هذه الأجهزة في بيئات صناعية أو تقنية تشغيلية التأكد من تعرضها وجدولة التحديث.

## ما يجب فعله الآن

1. حدّدوا أي وحدات RUGGEDCOM APE1808 تعمل بـ Fortinet NGFW في سجل الأصول لديكم.
2. خططوا لتحديث Fortigate NGFW إلى V7.6.9 أو أحدث وفق إجراء التحديث الآمن من Siemens.
3. تواصلوا مع دعم عملاء Siemens للحصول على تفاصيل التحديث.
4. قيّدوا الوصول إلى CLI والإدارة المحلية على هذه الأجهزة بالموظفين المصرّح لهم فقط.
5. وثّقوا التغيير ضمن إجراءات إدارة التغيير للتقنية التشغيلية.