

CISA تحذّر من ثغرة حقن أوامر في SiteGuard Server Edition (EG Secure Solutions (CVE-2026-106931



أدرجت CISA ثغرة حقن أوامر نظام التشغيل CVE-2026-106931 في SiteGuard Server Edition، وقد تتيح للمهاجم تنفيذ أوامر بصلاحيات root أو SYSTEM. يُنصح بتطبيق إجراءات المورّد ومراجعة التعرّض.

- CVE-2026-106931 ثغرة حقن أوامر نظام التشغيل في EG Secure Solutions SiteGuard Server Edition.
- قد يتيح استغلالها الناجح تنفيذ أوامر اعتباطية بصلاحيات root أو SYSTEM على النظام المضيف.
- تشترط CISA تطبيق إجراءات التخفيف وفق تعليمات المورّد، بما يتوافق مع BOD 26-04 ومتطلبات الفرز الجنائي.
- إذا لم تتوفر إجراءات التخفيف، فإنّ إشاد CISA هو التوقف عن استخدام المنتج.
- الموعد النهائي للجهات الفيدرالية الأمريكية 23-10-2026، وعلى كل جهة تقييم تعرّض أصولها

أضافت CISA الثغرة CVE-2026-106931 إلى قائمتها للثغرات، وهي ثغرة حقن أوامر نظام التشغيل في منتج EG Secure Solutions SiteGuard Server Edition.

ما الذي تتيحه الثغرة

وفق المصدر، قد يتمكن المهاجم الذي يستغل الثغرة من تنفيذ أوامر اعتباطية على نظام التشغيل بصلاحيات root أو SYSTEM على النظام الذي يعمل عليه المنتج. ويعني هذا المستوى من الصلاحيات أن الخادم نفسه قد يتأثر كاملاً، لا التطبيق وحده.

ما الذي تطلبه CISA

تطلب CISA من الجهات تطبيق إجراءات التخفيف وفق تعليمات المورد، واتباع إرشادات BOD 26-04 الخاصة بترتيب أولويات التحديثات الأمنية بحسب المخاطر، كما تشير إلى متطلبات الفرز الجنائي (Forensics Triage Requirements). وإذا لم تتوفر إجراءات التخفيف فالإرشاد هو التوقف عن استخدام المنتج. أما الخدمات السحابية فُتتبع بشأنها إرشاد BOD 26-04 المعني. والموعد النهائي للجهات الفيدرالية هو 23-10-2026.

ويحمل المصدر كل جهة مسؤولية تقييم تعرّض كل أصل للإنترنت والالتزام بإرشادات التحديث. ولا يذكر المصدر الإصدارات المتأثرة ولا الإصدارات المصحّحة، لذا ينبغي التأكد منها مباشرة مع المورد.

نظرة عملية للمؤسسات في المملكة

ينطبق الموعد النهائي على الجهات الفيدرالية الأمريكية، لكن الإرشاد معيار مناسب لأي مؤسسة منظّمة تشغل هذا المنتج. والخطوة الأولى هي تحديد ما إذا كان SiteGuard Server Edition موجوداً في بيئتك وما إذا كان متاحاً من الإنترنت.

ما يجب فعله الآن

1. مراجعة سجل الأصول وأدوات الفحص بحثاً عن أي نشر لـ SiteGuard Server Edition.
2. تحديد النسخ المتاحة من الإنترنت ومنحها الأولوية.
3. التواصل مع EG Secure Solutions للحصول على تعليمات التخفيف وتفاصيل الإصدارات المتأثرة وتطبيقها.
4. عند عدم توفر إجراء تخفيف، التخطيط للتوقف عن استخدام المنتج كما ترشد CISA.
5. مراجعة السجلات وحفظ الأدلة على الخوادم المكشوفة لدعم الفرز الجنائي عند الاشتباه باختراق.