

CISA تضيف ست ثغرات مستغلة فعليًا إلى كتالوج KEV، منها ثغرات في Plex وSiteGuard وSiemens



أضافت CISA ست ثغرات في Plex Media Server وSiteGuard Server Edition من EG Secure إلى كتالوج KEV لوجود أدلة على استغلالها فعليًا، وتحث جميع المؤسسات على إعطائها الأولوية.

- أُضيفت ست ثغرات إلى كتالوج KEV استنادًا إلى أدلة على استغلالها فعليًا.
- أربع منها في Plex Media Server: CVE-2026-96652 و CVE-2026-96654 و CVE-2026-96655 و CVE-2026-96656.
- الثغرة CVE-2026-106931 حقن أوامر نظام التشغيل في SiteGuard Server Edition، والثغرة CVE-2026-110936 عنصر مسار بحث غير مضبوط في Siemens Software Center.
- التوجيه BOD 26-04 ملزم للجهات الفيدرالية المدنية الأمريكية فقط، لكن CISA تشجع جميع المؤسسات على اعتماد إدارة ثغرات قائمة على المخاطر.

أضافت CISA ست ثغرات إلى كتالوج الثغرات المستغلة المعروفة (KEV) بعد توافر أدلة على استغلالها فعليًا. وتشير الوكالة إلى أن هذه الأنواع من الثغرات تُعدّ وسيلة هجوم متكررة لدى الجهات الخبيثة.

ما الذي أُضيف

- CVE-2026-96652 و CVE-2026-96655: تزوير طلبات من جهة الخادم (SSRF) في Plex Media Server
- CVE-2026-96654: معالجة غير سليمة لمخططات URI المشفرة في صفحة ويب، في Plex Media Server
- CVE-2026-96656: تحكم خارجي في اسم الملف أو مساره، في Plex Media Server
- CVE-2026-106931: حقن أوامر نظام التشغيل في SiteGuard Server Edition من EG Secure Solutions
- CVE-2026-110936: عنصر مسار بحث غير مضبوط في Siemens Software Center

لا يتضمن المصدر تفاصيل الإصلاحات أو الإصدارات المتأثرة، لذا يُرجع إلى نشرة كل مورّد للاطلاع عليها.

لماذا يهم الأمر خارج الجهات الأمريكية

يُلزم التوجيه التشغيلي الملزم BOD 26-04 الجهات الفيدرالية المدنية بإعطاء أولوية للمعالجة السريعة للثغرات المدرجة في KEV على الأصول المكشوفة للعامة، متى كان استغلالها يمنح سيطرة كاملة على الأصل. كما يحدد توقعات أساسية للتحقق مما إذا كان النظام قد اختُرق قبل تطبيق التصحيح. ورغم أن التوجيه يخص تلك الجهات فقط، تشجع CISA جميع المؤسسات على اعتماد إدارة ثغرات قائمة على المخاطر وإعطاء أولوية لثغرات كتالوج KEV.

مقاربة مقترحة

اعتبروا إدراج الثغرة في KEV مؤشرًا قويًا على استغلالها فعليًا. تحققوا من وجود المنتجات المتأثرة في بيئتكُم، بما في ذلك المواضيع الأقل ظهورًا مثل الأنظمة غير المعتمدة رسميًا أو محطات العمل الهندسية، ثم رتبوا المعالجة بحسب درجة التعرّض أولاً.

ما يجب فعله الآن

1. راجعوا سجلات الأصول بحثًا عن Plex Media Server و SiteGuard Server Edition من Siemens Software Center.
2. اطلعوا على نشرة كل مورّد وطبّقوا التصحيحات أو إجراءات التخفيف المتاحة، بدءًا بالأنظمة المكشوفة على الإنترنت.
3. إذا كان نظام متأثر مكشوفًا قبل التصحيح، فراجعوا السجلات وابحثوا عن مؤشرات اختراق.
4. أدرجوا متابعة كتالوج KEV ضمن عملية إدارة الثغرات وأعطوا الأولوية للثغرات المدرجة فيه.
5. أزيلوا برمجيات خوادم الوسائط غير الضرورية من شبكات المؤسسة أو اعزلوها.