ثغرة حرجة في Node.js Brotli تؤثر على Siemens Desigo CC وGridscale X (CVE-2026-111497)



أفادت CISA بتأثر Siemens Desigo CC V8 وV9 ومنتجين من Gridscale X بالثغرة الحرجة CVE-2026-111497 في Node.js Brotli (CVSS 9.8). أصدرت Siemens إصدارات مصححة وتوصي بالتحديث.

- الثغرة CVE-2026-111497 المعروفة بـ«Node2Shell» هي كتابة خارج الحدود في مفكك Brotli المضمّن في Node.js، بتقييم CVSS v3 قدره 9.8.
- قد تتيح لمهاجم عن بُعد إتلاف الذاكرة وربما تنفيذ تعليمات برمجية عشوائية.
- المنتجات المتأثرة: جميع إصدارات Desigo CC V8 وV9، وGridscale X DSA من 5.3 حتى ما دون 5.4، وGridscale X PSS®E دون الإصدار 36.8.0.
- أصدرت Node.js تحديثات أمنية في 21 أكتوبر 2026، وأصدرت Siemens إصدارات جديدة للمنتجات المتأثرة.

- تشمل القطاعات المذكورة التصنيع الحيوي والطاقة وتقنية المعلومات.

نشرت CISA إشعارًا حول تأثير ثغرة حرجة في Node.js على عدد من منتجات Siemens. الثغرة المسجلة برقم **CVE-2026-111497** والمعروفة باسم «Node2Shell» موجودة في مفكك Brotli المضمّن في Node.js.

المنتجات المتأثرة

تتمثل المشكلة في كتابة خارج الحدود قد تتيح لمهاجم عن بُعد إتلاف الذاكرة وربما تنفيذ تعليمات برمجية عشوائية، وتبلغ درجتها 9.8 وفق CVSS v3. وقد أصدرت Node.js تحديثات أمنية في 21 أكتوبر 2026.

منتجات Siemens المتأثرة:

- Desigo CC family V8، جميع الإصدارات
- Desigo CC family V9، جميع الإصدارات
- Gridscale X DSA، الإصدارات من 5.3 حتى ما دون 5.4
- Gridscale X PSS®E، الإصدارات الأقل من 36.8.0

ويذكر الإشعار قطاعات التصنيع الحيوي والطاقة وتقنية المعلومات ضمن القطاعات ذات الصلة.

الإجراء المطلوب

أصدرت Siemens إصدارات جديدة للمنتجات المتأثرة وتوصي بالتحديث إلى أحدث الإصدارات. على الجهات التي تشغّل Desigo CC لإدارة المباني أو Gridscale X في أعمال مرتبطة بالطاقة التحقق من وقوع منشآتها ضمن النطاقات المذكورة، وجدولة التحديث عبر إدارة التغيير المعتادة. لا يذكر المصدر استغلالاً فعليًا للثغرة، لذا يُعامل الأمر كأولوية عالية في التحديث لا كحالة طارئة، مع مراعاة ارتفاع درجة الخطورة.

ما يجب فعله الآن

1. حصر جميع نسخ Desigo CC V8/V9 وGridscale X DSA وPSS®E، بما في ذلك الموجودة في شبكات التقنية التشغيلية وأنظمة إدارة المباني.
2. مطابقة الإصدارات المثبتة مع النطاقات المتأثرة وتطبيق تحديثات Siemens إلى أحدث الإصدارات.
3. الحد من إتاحة الأنظمة المتأثرة على الشبكة لشرائح ومستخدمين موثوقين إلى حين التحديث.
4. توثيق التعرض والمعالجة في سجلات إدارة الثغرات ومخاطر التقنية التشغيلية.
5. الاستفسار من الموردين والمتكاملين عمّا إذا كانت برمجيات أخرى لديكم تضمّن Node.js وتتأثر بالثغرة.