Siemens Mendix Studio Pro: ثغرات في MCP Server تتيح الوصول عن بُعد وهجمات CSRF



أفادت CISA بوجود ثغرتين في MCP Server ضمن Siemens Mendix Studio Pro 11 بدرجة CVSS v3 تبلغ 8.8. أصدرت Siemens إصدارات مصححة وتوصي بالتحديث إلى أحدث إصدار.

- ثغرتان هما CVE-2026-112136 وCVE-2026-112137 تؤثران على MCP Server في Mendix Studio Pro.
- الضعفان هما الارتباط بعنوان IP غير مقيَّد وتزوير الطلبات عبر المواقع (CSRF).
- الإصدارات المتأثرة: Mendix Studio Pro 11 من 11.15.0 وحتى ما دون 11.16.0، والإصدار 11.12 من 11.12.6 وحتى ما دون 11.12.7.
- قد يؤدي الاستغلال إلى وصول غير مصرح به إلى البيانات أو تنفيذ أدوات أو اختراق النظام.
- أصدرت Siemens إصدارات جديدة وتوصي بالتحديث إلى الأحدث.

نشرت CISA إشعارًا بشأن Siemens Mendix Studio Pro يتناول ثغرتين في مكوّن MCP Server. وتبلغ درجة CVSS v3 التي حددها المورّد 8.8.

ما الذي تأثر

تتعلق الثغرة الأولى CVE-2026-112136 بعدم تقييد MCP Server للمستمع HTTP بواجهة loopback كما ينبغي، مما قد يجعله متاحًا للأنظمة البعيدة. أما الثانية CVE-2026-112137 فهي ضعف من نوع تزوير الطلبات عبر المواقع (CSRF) قد يتيح لمهاجم خداع متصفح المستخدم لإرسال طلبات غير مصرح بها.

وبحسب الإشعار، يمكن لمهاجم لديه وصول إلى الشبكة التفاعل مع الخادم عن بُعد، وقد ينتج عن ذلك وصول غير مصرح به إلى البيانات أو تنفيذ أدوات أو اختراق النظام.

الإصدارات المتأثرة:

- Mendix Studio Pro 11: من 11.15.0 وحتى ما دون 11.16.0
- Mendix Studio Pro 11.12: من 11.12.6 وحتى ما دون 11.12.7

وتحدد CISA القطاعات المتأثرة بالتصنيع الحرج والطاقة، مع انتشار عالمي، ومقر Siemens في ألمانيا.

الإجراء المقترح

أصدرت Siemens إصدارات جديدة من المنتجات المتأثرة وتوصي بالتحديث إلى الأحدث. وينبغي للجهات التي تستخدم Mendix Studio Pro، خصوصًا لبناء تطبيقات للبيئات الصناعية أو التشغيلية، التأكد من الإصدارات التي يعمل بها مطوّروها وجدولة التحديث ضمن إجراءات إدارة التغيير المعتمدة.

ما يجب فعله الآن

1. حصر تثبيتات Mendix Studio Pro وتحديد ما يقع ضمن نطاقات الإصدارات المتأثرة.
2. التحديث إلى أحدث إصدار من Siemens وفق إجراءات إدارة التغيير.
3. التحقق من إمكانية الوصول إلى MCP Server من أجهزة أخرى، وتقييد الوصول الشبكي إلى محطات المطورين قدر الإمكان.
4. تنبيه المطورين إلى تجنب تصفح مواقع غير موثوقة أثناء تشغيل Studio Pro إلى حين التحديث.
5. توثيق التعرض والمعالجة في سجل إدارة الثغرات.