مكتبة Siemens .NET Client لواجهة SIMATIC S7 Webserver API: ثغرتان وتوصية بالتحديث



أفادت CISA بوجود ثغرتين في مكتبة Siemens .NET Client لواجهة SIMATIC S7 Webserver API قد تتيحان كشف معلومات حساسة أو كتابة ملفات خارج مجلد التنزيل. وتوصي Siemens بالتحديث.

- ثغرتان: CVE-2026-85114 وCVE-2026-85115.
- نوعا الضعف: اجتياز المسار (Path Traversal) ورسائل خطأ تتضمن معلومات حساسة.
- درجة CVSS v3 المذكورة: 7.5.
- الإصدارات المتأثرة: ما دون 3.3.61، وما دون 3.3.62 للإدخال الثاني.
- أصدرت Siemens إصدارًا جديدًا وتوصي بالتحديث إلى الأحدث.

نشرت CISA نشرة بشأن مكتبة Siemens .NET Client Library الخاصة بواجهة SIMATIC S7 Webserver API.

تتضمن المكتبة ثغرتين قد تتيحان للمهاجم الحصول على معلومات حساسة أو كتابة ملفات تعسفية خارج مجلد التنزيل المقصود.

ما الذي يتأثر

تذكر النشرة الإصدارات الأقل من 3.3.61 والأقل من 3.3.62، مع الإشارة إلى CVE-2026-85114 وCVE-2026-85115. وتوصف نقاط الضعف بأنها تقييد غير سليم لمسار الملف داخل مجلد محدد (Path Traversal)، وتوليد رسائل خطأ تتضمن معلومات حساسة. كما تُدرج درجة CVSS v3 بقيمة 7.5.

وفي حالة CVE-2026-85114، لا تتحقق التطبيقات المتأثرة تحققًا سليمًا من أسماء الملفات الواردة من خوادم بعيدة أثناء تنزيل التذاكر (tickets). ولذلك قد يتمكن مهاجم قادر على التلاعب باستجابة التذكرة من كتابة ملفات خارج الموقع المقصود.

وتصنّف النشرة المنتج ضمن قطاع التصنيع الحرج، وهو منتشر عالميًا، والشركة المصنعة يقع مقرها في ألمانيا.

النهج الموصى به

أصدرت Siemens إصدارًا جديدًا من المكتبة وتوصي بالتحديث إلى أحدث إصدار. وينبغي للجهات التي تطوّر أو تشغّل تطبيقات داخلية تعتمد على هذه المكتبة، خاصة في بيئات التقنية الصناعية والتشغيلية، أن تتحقق أولاً من استخدامها لها ومن الإصدار المثبّت، ثم تخطط للتحديث عبر إجراءات إدارة التغيير المعتادة.

لا تشير النشرة إلى استغلال فعلي للثغرتين، لذا يكفي نهج هادئ يقوم على الأولويات.

ما يجب فعله الآن

1. حصر التطبيقات والمشاريع التي تستخدم مكتبة .NET Client Library لواجهة SIMATIC S7 Webserver API وتسجيل إصداراتها.
2. تحديث التطبيقات المتأثرة إلى أحدث إصدار للمكتبة أصدرته Siemens.
3. اختبار التحديث في بيئة غير إنتاجية قبل نشره على الأنظمة المرتبطة ببيئة التقنية التشغيلية.
4. مراجعة ما إذا كانت التطبيقات تعرض رسائل خطأ مفصلة لمستخدمين غير موثوقين أو في السجلات.
5. توثيق الحالة والمعالجة في سجلات إدارة الثغرات ومخاطر التقنية التشغيلية.