CISA تحذّر من ثغرات حرجة في openPDC وopenHistoriang من Grid Protection Alliance



نشرت CISA نشرة تخص أنظمة التحكم الصناعي بشأن openPDC وopenHistoriang تتضمن عدة ثغرات بدرجة CVSS v3 تبلغ 9.8. على مشغّلي قطاع الطاقة تحديد الإصدارات المتأثرة وتحديثها.

- المتأثر: openPDC قبل الإصدارين 2.9.477 و2.9.482، وصورة Docker الخاصة به، openHistoriang قبل 2.8.580 و2.8.585.
- تذكر النشرة درجة CVSS v3 قدرها 9.8.
- تشمل أنواع الضعف إلغاء التسلسل غير الآمن، وغياب المصادقة لوظيفة حرجة، وSSRF، وبيانات اعتماد مضمّنة، والانعكاس غير الآمن.
- الثغرة CVE-2026-100730 تتعلق بواجهة خدمة تُلغي تسلسل بيانات يوفرها العميل؛ وعلى الأنظمة التي تستخدم مصادقة Windows يجب أن يكون المهاجم موثّقًا أولاً.
- تصنّف النشرة المنتجات ضمن قطاع الطاقة وتذكر انتشارها عالميًا.

نشرت CISA نشرة بشأن أنظمة التحكم الصناعي تخص openPDC وopenHistoriang، وهما برمجيتان من Grid Protection Alliance تُستخدمان في قطاع الطاقة. وتذكر النشرة درجة CVSS v3 قدرها 9.8.

ما الذي تأثر

تحدد النشرة إصدارات openPDC الأقدم من 2.9.477 و2.9.482، وصورة Docker الخاصة به ضمن النطاقات نفسها، وإصدارات openHistorian الأقدم من 2.8.580 و2.8.585. والثغرات المدرجة هي CVE-2026-104629 وCVE-2026-100730 وCVE-2026-105281 وCVE-2026-85479 وCVE-2026-101022، مع إضافة CVE-2026-105278 لصورة Docker.

وتتنوع أنواع الضعف بين إلغاء تسلسل بيانات غير موثوقة، وغياب المصادقة لوظيفة حرجة، وتزوير الطلبات من جهة الخادم (SSRF)، واستخدام بيانات اعتماد مضمّنة، والانعكاس غير الآمن.

ومن الأمثلة CVE-2026-100730: واجهة خدمة تُلغي تسلسل بنية بيانات يرسلها العميل. وعند استخدام مصادقة Windows يجب أن يكون المهاجم موثّقًا مسبقًا للوصول إلى هذه الوظيفة. والنص الذي راجعناه مقتطع، لذا يُنصح بقراءة نشرة CISA كاملة للاطلاع على بقية التفاصيل.

الإجراء المقترح

على الجهات التي تشغّل هذه المنتجات، خصوصًا في الطاقة وبيئات التقنية التشغيلية، التأكد من استخدامها وتحديد الإصدارات. وتتم مقارنة الإصدارات المثبّتة بالنطاقات المعالجة في النشرة، وجدولة التحديث عبر إدارة التغيير المعتادة. وإلى حين ذلك يُقيَّد الوصول الشبكي إلى واجهة الخدمة على من يحتاجه فقط.

ما يجب فعله الآن

1. مراجعة سجل الأصول للتحقق من وجود openPDC وصورة Docker وopenHistoriang وتسجيل الإصدارات المستخدمة.
2. مقارنة الإصدارات بالنطاقات المعالجة في نشرة CISA وجدولة التحديث عبر إدارة التغيير.
3. تقييد الوصول الشبكي إلى واجهة الخدمة على المسؤولين المصرّح لهم وعزلها عن الشبكات غير الموثوقة.
4. قراءة النشرة الكاملة بما فيها وصف كل ثغرة لمعرفة إجراءات التخفيف الإضافية غير التحديث.
5. مراجعة سجلات الأنظمة المتأثرة بحثًا عن وصول غير متوقع إلى واجهة الخدمة.