ثغرة حرجة CVE-2026-42810 في Apache Polaris تسمح بالوصول العابر للجداول عبر S3

حرجة - CVSS 9.9

CVE ID	CVE-2026-42810
درجة CVSS	9.9 (CRITICAL)
CWE	CWE-20
تاريخ النشر	2026-05-04 17:16:26

وصف الثغرة

Apache Polaris accepts literal `*` characters in namespace and table names. When it later builds temporary S3 access policies for delegated table access, those same characters appear to be reused unescaped in S3 IAM resource patterns and `s3:prefix` conditions. In S3 IAM policy matching, `*` is treated as a wildcard rather than as ordinary text. That means temporary credentials issued for one crafted table can match the storage path of a different table. In private testing against Polaris 1.4.0 using Polaris' AWS S3 temporary- credential path on both MinIO and real AWS S3, credentials returned for crafted tables such as `f*.t1`, `f*.*`, `*.*`, and `foo.*` could reach other tables' S3 locations. The confirmed behavior includes: - reading another table's metadata control file ([Iceberg metadata JSON]); - listing another table's exact S3 table prefix ([table prefix]); - and, when write delegation was returned for the crafted table, creating and deleting an object under another table's exact S3 table

prefix. A control case using ordinary different names did not allow the same cross-table access. A least-privilege AWS S3 variant was also confirmed in which the attacker principal had no Polaris permissions on the victim table and only the minimal permissions required to create and use a crafted wildcard table (namespace-scoped `TABLE_CREATE` and `TABLE_WRITE_DATA` on `*`). In that setup, direct Polaris access to `foo.t1` remained forbidden, but the attacker could still create and load `*.*`, receive delegated S3 credentials, and use those credentials to list, read, create, and delete objects under `foo.t1`. In Iceberg, the metadata JSON file is a control file: it tells readers which data files belong to the table, which snapshots exist, and which table version to read. So unauthorized access to it is already a meaningful confidentiality problem. The confirmed write-capable variant means the issue is not limited to disclosure.

التحليل والتوصيات

◎نظرة عامة على الثغرة CVE-2026-42810

كشفت مؤسسة Apache Software Foundation عن ثغرة أمنية حرجة في منصة **Apache Polaris**، وهي كتالوج بيانات مفتوح المصدر يُستخدم على نطاق واسع مع تنسيق جداول *Apache Iceberg* لإدارة بحيرات البيانات (Data Lakes) في البيئات السحابية. حملت الثغرة المعرّف **CVE-2026-42810** وحصلت على درجة خطورة مرتفعة للغاية تبلغ **9.9 من 10** وفقاً لمعيار CVSS v3.1، ما يضعها في الفئة **الحرجة**.

تنبع الثغرة من قبول Apache Polaris للحرف الخاص (النجمة) داخل أسماء مساحات الأسماء (Namespaces) أو أسماء الجداول (Tables) دون تهريب (Escaping)، ثم إعادة استخدام هذه الأحرف في بناء سياسات IAM المؤقتة الخاصة بخدمة Amazon S3 عند

منح صلاحيات الوصول المفوّض (Delegated Access). وبما أن خدمة S3 IAM تعامل الرمز باعتباره بطاقة عمومية (Wildcard) وليس نصاً عادياً، فإن بيانات الاعتماد المؤقتة المميزة لجدول مصمم بعناية يمكن أن تطابق مسارات تخزين جداول أخرى تماماً.

◎تفاصيل تقنية دقيقة

تصنف الثغرة تحت **CWE-20: Improper Input Validation** (التحقق غير السليم من المدخلات). السيناريو الهجومي يتم على النحو التالي:

- يقوم المهاجم بإنشاء جدول بأسماء تحتوي على أحرف بدل مثل `f*.t1` أو `.` أو `foo..`
- يطلب المهاجم بيانات اعتماد S3 مؤقتة عبر مسار التفويض الخاص بـ Polaris.
- يبني Polaris سياسة IAM مؤقتة تحتوي على أنماط موارد S3 وشروط `s3:prefix` تتضمن أحرف غير مهربة.
- نتيجة لذلك، تُقرأ هذه الأحرف كبطاقات عمومية، فتتمكن بيانات الاعتماد من الوصول إلى مسارات جداول أخرى لا يملك المهاجم أي صلاحيات عليها.

تم تأكيد السلوك الخطير التالي في بيئات اختبار خاصة على الإصدار **Polaris** **1.4.0**، سواء مع **AWS S3** أو **MinIO** الحقيقية:

1. **قراءة ملف التحكم metadata.json** الخاص بجدول Iceberg آخر، وهو ملف يحدد البيانات والسجلات الفعلية للجدول.
2. **سرد محتويات** المسار الدقيق لجدول ضحية عبر عملية List على S3.
3. **إنشاء وحذف كائنات** داخل مسار جدول الضحية عند منح صلاحيات الكتابة المفوّضة، مما يفتح الباب أمام هجمات إفساد البيانات (Data Corruption) أو الحذف الخبيث.

◎خطورة السيناريو ذي الامتيازات الأدنى

أخطر ما في هذه الثغرة هو تأكيد متغير هجومي يعتمد على مبدأ **أقل الامتيازات** (Least Privilege)؛ إذ يستطيع مهاجم لا يملك أي صلاحيات Polaris على جدول الضحية (`foo.t1`) — وإنما فقط الصلاحيات الدنيا TABLE_CREATE وTABLE_WRITE_DATA على مستوى مساحة الأسماء — أن ينفذ ما يلي:

- إنشاء جدول احتيالي بالاسم ..
- استلام بيانات اعتماد S3 المفوّضة.
- استخدام هذه البيانات لسرد وقراءة وإنشاء وحذف الكائنات داخل مسار `foo.t1` مباشرة.

هذا يعني أن نموذج التحكم بالوصول في Polaris يتم تجاوزه بشكل كامل عبر خدمة S3 ذاتها، حتى لو كانت قواعد Polaris الداخلية ترفض الوصول المباشر.

◎الأنظمة والإصدارات المتأثرة

- **Apache Polaris** الإصدار 1.4.0 (مؤكد).
- الإصدارات الأقدم التي تستخدم نفس آلية بناء سياسات IAM المؤقتة لـ S3.
- جميع عمليات النشر التي تعتمد على **AWS S3** أو **MinIO** أو أي تخزين كائنات متوافق مع S3 يدعم نمط IAM Wildcards.
- البيئات التي تستخدم Polaris كطبقة كتالوج لجداول **Apache Iceberg**.

◎الأثر على مزودي الاستضافة ومراكز البيانات في المملكة

مع التوسع الكبير في تبني بحيرات البيانات (Data Lakehouse) في المملكة العربية السعودية ضمن مبادرات **رؤية المملكة 2030** والتحول الرقمي للجهات الحكومية والقطاع المالي، أصبحت منصات مثل Apache Iceberg وApache Polaris مكوناً أساسياً في البنية التحتية لكثير من الشركات. هذه الثغرة تمثل تهديداً مباشراً لـ:

- مراكز البيانات المحلية المرخصة من **هيئة الاتصالات والفضاء والتقنية (CST)** سابقاً **CITC**.
- مزودي الخدمات السحابية المحلية مثل **STC Cloud** و**Mobily Business** و **Sahara Net**.
- الجهات المالية الخاضعة لإشراف **البنك المركزي السعودي (SAMA)**، وإطار **SAMA Cyber Security Framework**.
- الجهات الحكومية الملتزمة بـ**الضوابط الأساسية للأمن السيبراني (NCA)** الصادرة عن **الهيئة الوطنية للأمن السيبراني (ECC)**.
- المؤسسات التي تعالج بيانات شخصية خاضعة لـ**نظام حماية البيانات الشخصية (PDPL)**.

أي تسرب أو عبث ببيانات الجداول قد يمثل حادثة أمن سيبراني يستوجب التبليغ عنها وفقاً لإلزامات NCA وSAMA، وقد يعرض الشركة لغرامات بموجب PDPL تصل إلى ملايين الريالات.

◎مؤشرات الاختراق المحتملة (IoCs)

- وجود جداول أو مساحات أسماء تحتوي على الحرف في كتالوج Polaris.
- طلبات `GetSubscopedCredentials` لجداول غير معتادة الأسماء.
- سجلات **AWS CloudTrail** تُظهر عمليات `ListObjectsV2`, `GetObject`, `PutObject`, `DeleteObject` من Session Tokens مؤقتة على مسارات لا تتطابق

.مع الجدول الأصلي

- تعديلات غير مبررة على ملفات `metadata.json` أو اختفاء لقطات Iceberg (Snapshots).

◎خطوات الاستجابة الموصى بها لمدراء الأنظمة

1. الإجراءات الفورية (خلال 24 ساعة)

- تطبيق التصحيحات الأمنية الصادرة عن Apache Polaris فور توفرها ومراجعة القائمة البريدية الرسمية.
- تدقيق كتالوج Polaris للبحث عن أي أسماء جداول أو مساحات أسماء تحتوي على * أو أحرف خاصة.
- تعطيل مسار التفويض الخاص بصلاحيات S3 المؤقتة مؤقتاً إذا لم يكن مستخدماً بشكل حرج.

2. التحقق من السياسات (خلال 72 ساعة)

- مراجعة قواعد سياسات IAM المستخدمة في Polaris والتأكد من أن أي إدخال يمر عبر آلية تهريب صارمة.
- تفعيل **S3 Access Logs** و**CloudTrail Data Events** على جميع حاويات S3 المرتبطة بجداول Iceberg.
- تطبيق سياسات **Bucket Policy** و**SCP** تمنع الوصول عبر Session Tokens إلى مسارات خارج النطاق الأصلي.

3. تعزيزات طويلة الأمد

- فرض قائمة بيضاء (Whitelist) لأحرف أسماء الجداول تسمح فقط بالأحرف الأبجدية الرقمية والشرطة السفلية.

- فصل حاويات S3 لكل مستأجر (Tenant) أو مساحة أسماء حساسة.
- تطبيق تشفير مفاتيح مختلفة (KMS CMK) لكل جدول حساس لمنع الوصول العابر حتى لو تم تجاوز السياسات.
- دمج المراقبة مع **SIEM** ومراكز العمليات الأمنية SOC، ورفع التنبيهات للجنة الأمن السيبراني وفق متطلبات NCA.

◎دور 4jawaly في دعم المؤسسات السعودية

باعتبارها شركة سعودية مرخصة من هيئة الاتصالات والفضاء والتقنية (ترخيص 291-10-32) وحاصلة على شهادة **ISO 27001**، تقدم **فورجوالي (4jawaly)** حلولاً متكاملة تساعد الجهات في مواجهة مثل هذه الحوادث، منها:

- **خدمات الإشعارات الفورية عبر SMS** لتنبيه فرق الأمن عند اكتشاف نشاط مشبوه في بيئات S3 وIceberg.
- **تكامل WhatsApp Business API** لإرسال تقارير الحوادث إلى مسؤولي تقنية المعلومات في الوقت الحقيقي.
- **روبوتات الدردشة الذكية** لدعم فرق الاستجابة للحوادث وتوفير إرشادات فورية.
- **خدمات الاستضافة الآمنة** في مراكز بيانات داخل المملكة متوافقة مع متطلبات توطين البيانات.

◎خاتمة

تعد ثغرة **CVE-2026-42810** تذكيراً حاداً بأن التحقق من المدخلات ليس مجرد ممارسة جيدة، بل خط دفاع أول حاسم. مع دمج Polaris المتزايد في البنى التحتية للبيانات في المملكة، يجب على كل مدير نظام وفريق DevSecOps معاملة هذه الثغرة كأولوية قصوى، وتطبيق التصحيحات فور صدورها، ومراجعة نماذج التفويض المفوّض لـ S3 بشكل شامل. التكلفة المحتملة للتجاهل قد تتجاوز بكثير تكلفة التصحيح،

خاصة في ظل التشريعات الصارمة مثل PDPL وECC.

الأسئلة الأكثر شيوعاً

ما هي ثغرة CVE-2026-42810 بشكل مبسط؟

هي ثغرة حرجة في Apache Polaris تسمح للمهاجم بإنشاء جداول بأسماء تحتوي على حرف النجمة (*)، ما يؤدي إلى منح بيانات اعتماد S3 مؤقتة تصل إلى بيانات جداول أخرى لا يملك صلاحيات عليها.

هل إصدار Apache Polaris الذي نستخدمه متأثر؟

تم تأكيد التأثير على الإصدار 1.4.0 والإصدارات الأقدم التي تستخدم نفس آلية بناء سياسات IAM المؤقتة. يجب مراجعة الإعلان الرسمي من Apache والتحديث للإصدار المصحح فور صدوره.

ما الإجراء الأعجل الذي يجب اتخاذه الآن؟

تدقيق كتالوج Polaris فوراً للبحث عن أي أسماء جداول أو مساحات أسماء تحتوي على حرف (*)، وتعطيل مسار التفويض المؤقت لـ S3 مؤقتاً، وتفعيل CloudTrail وS3 Access Logs لرصد أي نشاط مشبوه.

كيف تؤثر هذه الثغرة على الامتثال لأنظمة NCA وSAMA وPDPL؟

أي تسرب لبيانات الجداول يعد حادثة أمن سيبراني يستوجب التبليغ عنها وفق إطار NCA ECC وSAMA CSF، وقد يعرض المؤسسة لغرامات PDPL إذا شملت البيانات معلومات شخصية.

هل يكفي تطبيق التصحيح أم أحتاج إجراءات إضافية؟

التصحيح ضروري لكنه غير كافٍ. يجب فرض قائمة بيضاء لأحرف أسماء الجداول، وفصل حاويات S3 لكل مستأجر، واستخدام مفاتيح KMS منفصلة لكل جدول حساس، ودمج المراقبة مع منظومة SIEM.

مقالات ذات صلة

مشاهدة المزيد

تنبيهات أمنية

ثغرة حرجة CVE-2026-42809 في Apache Polaris: تسريب بيانات اعتماد التخزين المؤقتة عبر مسارات جداول مُتحكّم بها

تُتيح بيانات اعتماد التخزين المؤقتة في Apache Polaris (CVE-2026-42809) بتسريب بيانات اعتماد التخزين المؤقتة عبر مسارات جداول مُتحكّم بها. دليل المعالجة لمديري الأنظمة في السعودية.

إقرأ المزيد

تنبيهات أمنية

ثغرة CVE-2026-4803 في إضافة Royal Elementor Addons لـ WordPress: حقن سكربتات مُخزّنة عبر طلبات AJAX غير مُوثّقة

تحذير أمني: ثغرة CVE-2026-4803 في إضافة Royal Elementor Addons لـ WordPress تسمح بحقن سكربتات. خطوات الحماية لمسؤولي الاستضافة السعودية.

إقرأ المزيد

تنبيهات أمنية

ثغرة حقن SQL حرجة في إضافة WeePie Cookie Allow لـ WordPress (CVE-2026-4304)

ثغرة حرجة CVE-2026-4304 في إضافة WeePie Cookie Allow لـ WordPress تُهدد المواقع السعودية. تعرّف على التفاصيل وخطوات الحماية الفورية.

إقرأ المزيد
