# CVE-2026-42812: ثغرة أمنية حرجة في Apache Iceberg

**حرجة - CVSS 9.9**

| | |
|---|---|
| **CVE ID** | CVE-2026-42812 |
| **درجة CVSS** | 9.9 (CRITICAL) |
| **CWE** | CWE-20 |
| **تاريخ النشر** | 2026-05-04 17:16:26 |

## وصف الثغرة

In Apache Iceberg, the table's metadata files are control files: they tell readers which data files belong to the table and which table version to read. `write.metadata.path` is an optional table property that tells Polaris where to write those metadata files. For a table already registered in a Polaris-managed catalog, changing only that property through an `ALTER TABLE`-style settings change (not a row-level `INSERT`, `SELECT`, `UPDATE`, or `DELETE`) bypasses the commit-time branch that is supposed to revalidate storage locations. The full persisted / credential-vending variant requires the affected catalog to have `polaris.config.allow.unstructured.table.location=true`, with `allowedLocations` broad enough to include the attacker-chosen target. `allowedLocations` is the admin-configured allowlist of storage paths that the catalog is allowed to use. Public project materials suggest that this flag is a real supported compatibility / layout mode, not just a contrived lab-only prerequisite. In that

configuration, a user who can change table settings can cause Apache Polaris itself to write new table metadata to an attacker-chosen reachable storage location before the intended location-validation branch runs. If the later concrete-path validation also accepts that location, Polaris persists the resulting metadata path into stored table state. Later table-load and credential APIs can then return temporary cloud-storage credentials for the same location without revalidating it. In plain terms, Polaris can later hand out temporary storage access for the same attacker-chosen area. That attacker-chosen area does not need to be limited to the poisoned table's own files. If it is a broader storage prefix, another table's prefix, or, depending on configuration or provider behavior, even a bucket/container root, the resulting disclosure or corruption scope can extend to any data and metadata Polaris can reach there. The practical consequences are therefore similar to the staged-create credential-vending issue already discussed: data and metadata reachable in that storage scope can be exposed and, if write-capable credentials are later issued, modified, corrupted, or removed. Even before that later credential step, Polaris itself performs the metadata write to the unchecked location. So the core issue is not only later credential vending. The primary defect is that Polaris skips its intended location checks before performing a security-sensitive metadata write when only `write.metadata.path` changes. When `polaris.config.allow.unstructured.table.location=false`, current code review suggests the later `updateTableLike(...)` validation usually rejects out-of-tree metadata locations before the unsafe path is persisted. That may reduce the persisted / credential-vending variant, but it does not prevent the underlying defect: Polaris still skips the intended pre-write location check when only `write.metadata.path` changes.

## التحليل والتوصيات

## ◎مقدمة

تم اكتشاف ثغرة أمنية حرجة في Apache Iceberg، وهي مكتبة تستخدم لقراءة وكتابة البيانات في أنظمة تخزين البيانات الضخمة. هذه الثغرة، المعروفة باسم CVE-2026-42812، يمكن أن تسمح للمهاجمين بكتابة ملفات بيانات إلى مواقع تخزين غير مصرح بها، مما قد يؤدي إلى تسرب البيانات أو تلفها.

## ◎تفاصيل الثغرة

تحدث الثغرة بسبب خاصية `write.metadata.path` التي تسمح للمستخدمين بتحديد موقع ملفات البيانات. عندما يتم تغيير هذه الخاصية من خلال تعديل إعدادات الجدول، يتم تجاوز التحقق من صحة موقع التخزين، مما يسمح للمهاجمين بكتابة ملفات البيانات إلى مواقع غير مصرح بها.

## ◎الأنظمة المتأثرة

تأثر جميع الإصدارات الحالية من Apache Iceberg بهذه الثغرة. يُشجع المستخدمون على التحديث إلى الإصدار الأخير من المكتبة لتجنب هذه الثغرة.

## ◎خطوات التصحيح

للمسؤولين في السعودية، يُشجع على اتباع الخطوات التالية لتصحيح هذه الثغرة:

- تحديث Apache Iceberg إلى الإصدار الأخير.
- تأكيد أن خاصية `polaris.config.allow.unstructured.table.location` معطلة.

- تأكيد أن قائمة المواقع المسموح بها (`allowedLocations`) محددة بشكل صحيح.

### ◎سياق السعودية

هذه الثغرة تثير قلقًا خاصًا في السعودية، حيث أن العديد من الشركات والمؤسسات تستخدم Apache Iceberg في أنظمتها. يُشجع المسؤولون على اتخاذ إجراءات فورية لتصحيح هذه الثغرة وتجنب أي مخاطر أمنية.

### ◎مخاطر الاستغلال

تُعتبر هذه الثغرة حرجة، ويمكن أن تؤدي إلى تسرب البيانات أو تلفها. يُشجع المستخدمون على اتخاذ إجراءات فورية لتصحيح هذه الثغرة وتجنب أي مخاطر أمنية.

## الأسئلة الأكثر شيوعًا

#### ما هي الثغرة الأمنية في Apache Iceberg؟

ثغرة أمنية حرجة يمكن أن تسمح للمهاجمين بكتابة ملفات بيانات إلى مواقع تخزين غير مصرح بها.

#### كيف يمكن تصحيح هذه الثغرة؟

يمكن تصحيح هذه الثغرة عن طريق تحديث Apache Iceberg إلى الإصدار الأخير وتأكيد أن خاصية `polaris.config.allow.unstructured.table.location` معطلة.

### ما هي المخاطر الناجمة عن هذه الثغرة؟

تُعتبر هذه الثغرة حرجة، ويمكن أن تؤدي إلى تسرب البيانات أو تلفها.

## مقالات ذات صلة

مشاهدة المزيد

تنبيهات أمنية

CVE-2026-42811: ثغرة أمنية حرجة في Apache Polaris

CVE-2026-42811: ثغرة أمنية حرجة في Apache Polaris تتيح للمهاجمين الحصول على أذونات وصول موسعة إلى البيانات المخزنة في سلة Google Cloud Storage.

إقرأ المزيد

تنبيهات أمنية

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

ثغرة CVE-2026-42810 الحرجة في Apache Polaris تسمح بالوصول العابر لجداول Iceberg عبر S3. تعرف على الحل وخطوات الحماية للمؤسسات السعودية.

إقرأ المزيد

تنبيهات أمنية

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

ثغرة حرجة 9.9 في Apache Polaris (CVE-2026-42809) تُتيح تسريب بيانات اعتماد التخزين. دليل المعالجة لمديري الأنظمة في السعودية.

[إقراء المزيد]

---

تم إنشاء هذا التقرير تلقائيًا بواسطة نظام CVE Watcher - 4Jawaly

رابط المقال: https://www.4jawaly.com/ar/post/cve-2026-42812-apache-iceberg/