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

حرجة - CVSS 9.9

CVE ID	CVE-2026-42811
درجة CVSS	9.9 (CRITICAL)
CWE	CWE-20
تاريخ النشر	2026-05-04 17:16:26

وصف الثغرة

In plain terms, Apache Polaris is supposed to issue short-lived GCS credentials that only work for one table's files, but a crafted namespace or table name can cause those credentials to work across the configured bucket instead. Apache Polaris builds Google Cloud Storage downscoped credentials by creating a Credential Access Boundary (CAB) with CEL conditions that are intended to restrict access to the requested table's storage path. The relevant CEL string is built from the bucket name and the table path. That table path is derived from namespace and table identifiers. In current code, that path appears to be inserted into the CEL expression without escaping. As a result, a namespace or table identifier containing a single quote and other URI-safe CEL fragments can break out of the intended quoted string and change the meaning of the CEL condition. In private testing against Polaris 1.4.0 on real Google Cloud Storage, it was confirmed that Polaris accepted a crafted identifier and returned delegated GCS

credentials whose CEL path restriction had effectively collapsed. Those delegated credentials could then: - list another table's object prefix; - read another table's metadata control file (Iceberg metadata JSON); - create and delete an object under another table's object prefix; - and also list, read, create, and delete objects under an unrelated external prefix in the same bucket that was not part of any table path. That last point is important. The issue is not limited to "another table". In the confirmed setup, once Apache Polaris returned credentials for the crafted table, the path restriction inside the configured bucket was effectively gone. The practical effect is that temporary credentials for one crafted table can be broader than the table Polaris was asked to authorize, and can become effectively bucket-wide within the configured bucket. The current GCS testing used a Polaris principal with broad catalog privileges for setup. A separate least-privilege Polaris RBAC variant has not yet been tested on GCS. However, the storage-credential broadening behavior itself has been confirmed on GCS.

التحليل والتوصيات

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

تم اكتشاف ثغرة أمنية حرجة في Apache Polaris، وهي أداة تستخدم لتحديد نطاق بيانات التخزين في Google Cloud Storage. الثغرة، المعروفة باسم CVE-2026-42811، تتيح للمهاجمين الحصول على أذونات وصول موسعة إلى البيانات المخزنة في سلة Google Cloud Storage.

تحدث الثغرة بسبب طريقة بناء شروط وصول الأذونات في Apache Polaris. عندما يتم إنشاء أذونات وصول مؤقتة، يتم بناء شروط وصول الأذونات باستخدام تعبيرات

CEL (Common Expression Language). ومع ذلك، يتم إدراج مسار الجدول في التعبير CEL دون حماية، مما يسمح للمهاجمين بخرق الحماية وزيادة نطاق الوصول.

يمكن للمهاجمين استخدام هذه الثغرة للوصول إلى بيانات أخرى في سلة Google Cloud Storage، بما في ذلك قراءة وكتابة بيانات الجداول الأخرى. بالإضافة إلى ذلك، يمكنهم إنشاء وحذف كائنات في مسار الجدول الآخر.

الأنظمة المتأثرة

تأثر الثغرة الإصدارات التالية من Apache Polaris:

- Apache Polaris 1.4.0

الإجراءات الموصى بها

نوصي مسؤولي الاستضافة في السعودية باتخاذ الإجراءات التالية:

1. تحديث Apache Polaris إلى الإصدار الأخير
2. مراجعة أذونات الوصول إلى سلة Google Cloud Storage
3. تطبيق سياسات أمان صارمة لمنع الوصول غير المصرح به إلى البيانات

السياق السعودي

تعتبر الثغرة الأمنية في Apache Polaris تهديداً كبيراً لأمان البيانات في السعودية. نظراً لاستخدام العديد من الشركات السعودية لخدمات Google Cloud Storage، فإن الثغرة يمكن أن تؤثر على أمان البيانات الحساسة.

نوصي مسؤولي الاستضافة في السعودية بالعمل مع هيئة الاتصالات وتقنية المعلومات (CITC) لضمان تطبيق سياسات أمان صارمة ومراجعة أذونات الوصول إلى البيانات.

مخاطر الاستغلال

تعتبر الثغرة الأمنية في Apache Polaris خطراً كبيراً لأمان البيانات. يمكن للمهاجمين استخدام الثغرة لسرقة البيانات الحساسة أو تدميرها.

نوصي مسؤولي الاستضافة في السعودية بالعمل بسرعة لتحديث Apache Polaris وتطبيق سياسات أمان صارمة لمنع الاستغلال.

الأسئلة الأكثر شيوعاً

ما هي الثغرة الأمنية في Apache Polaris؟

الثغرة الأمنية في Apache Polaris هي ثغرة تتيح للمهاجمين الحصول على أذونات وصول موسعة إلى البيانات المخزنة في سلة Google Cloud Storage.

كيف يمكنني حماية بياناتي من الثغرة الأمنية في Apache Polaris؟

يمكنك حماية بياناتك من الثغرة الأمنية في Apache Polaris عن طريق تحديث Apache Polaris إلى الإصدار الأخير ومراجعة أذونات الوصول إلى سلة Google Cloud Storage.

ما هي مخاطر الاستغلال للثغرة الأمنية في Apache Polaris؟

مخاطر الاستغلال للثغرة الأمنية في Apache Polaris هي سرقة البيانات الحساسة أو تدميرها.

مقالات ذات صلة

مشاهدة 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.

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
