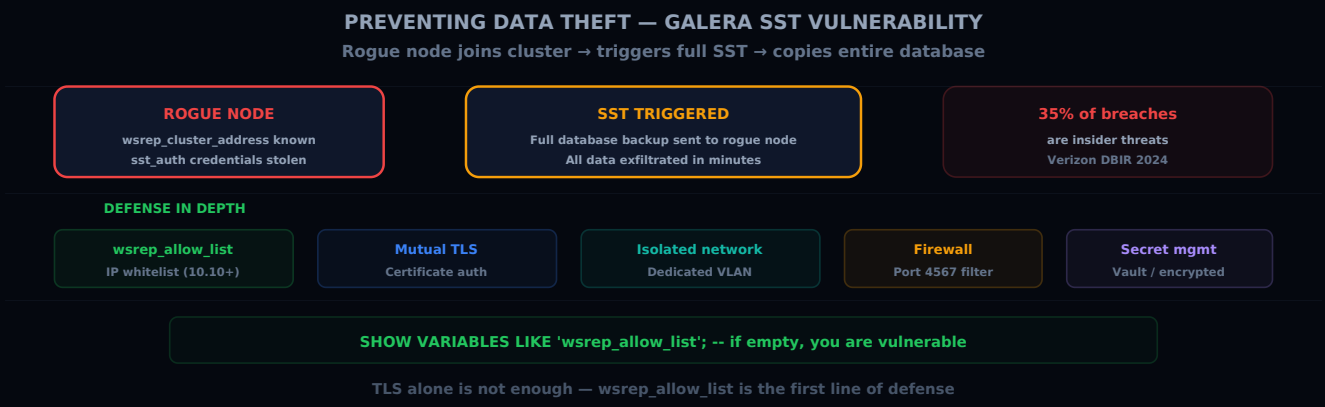
منع سرقة البيانات: طبعة Galera

Sylvain ARBAUDIE · 12 مارس 2025

GALERA MARIADB SECURITY SST



السيناريو الكابوس

تخيل: قام أحد المهاجمين بتكوين خادم MariaDB باستخدام معلمات wsrep الصحيحة، وتعرف عنوان المجموعة Galera وكلمة مرور SST. ينضم إلى الكتلة. يكتشف Galera عقدة جديدة لا تحتوي على بيانات ويقوم بتشغيل **State Snapshot Transfer (SST)** — نقل كامل لجميع البيانات الموجودة في المجموعة إلى العقدة المهاجمة.

وفي غضون دقائق قليلة (أو ساعات حسب حجم قاعدة البيانات)، يحصل المهاجم على نسخة كاملة من قاعدة البيانات الخاصة بك. لا يوجد حقن SQL، ولا يوجد استغلال لثغرة التطبيق. مجرد الانضمام إلى المجموعة باستخدام بيانات الاعتماد الصحيحة.

إنه ليس خيالاً علمياً. وفقاً لتقرير Verizon 2024 لخرق البيانات، **35% من خروقات البيانات تنطوي على تهديدات داخلية** - الموظفين أو المقاولين أو الأشخاص الذين لديهم وصول مشروع إلى البنية التحتية.

كيف يعمل SST

نقل لقطة الحالة هو الآلية التي من خلالها يقوم Galera بتهيئة عقدة جديدة. عندما تنضم عقدة إلى المجموعة بدون بيانات (أو ببيانات قديمة جداً بحيث لا تتناسب مع IST تزايدي)، تقوم المجموعة بتشغيل SST:

1. تم تحديد العقدة المانحة (عضو موجود في المجموعة).

2. يقوم المانح بإجراء نسخة احتياطية كاملة (عبر mariackup أو rsync أو mysqldump)
3. يتم إرسال النسخة الاحتياطية إلى عقدة الانضمام عبر الشبكة
4. تقوم عقدة الانضمام باستعادة النسخة الاحتياطية والانضمام إلى المجموعة

المشكلة: **افتراضياً، يمكن لأي عقدة تحتوي على معلومات المجموعة الصحيحة تشغيل SST** . لا توجد قائمة بيضاء، ولا يوجد تحقق من هوية عقدة الانضمام.

الحد الأدنى من التكوين للهجوم

ما يحتاجه المهاجم:

```
[mysqld]
wsrep_cluster_address = gcomm://10.0.1.10,10.0.1.11,10.0.1.12
wsrep_sst_method = mariabackup
wsrep_sst_auth = sst_user:sst_password
```

ثلاث أجزاء من المعلومات: عنوان المجموعة وأسلوب SST وبيانات اعتماد SST. في العديد من المؤسسات، يتم تخزين هذه المعلومات في ملفات تكوين غير مشفرة، أو أدلة تشغيل Ansible غير مشفرة، أو مستودعات Git الخاصة.

لماذا لا يكفي TLS

"لكننا نستخدم TLS لحركة مرور Galera!" — وهذا اعتراض متكرر. وهذا غير كاف.

يقوم TLS بتشفير حركة المرور بين العقد، لكنه لا يتحقق بالضرورة من هوية العقدة المنضمة. حتى مع TLS، إذا كان لدى المهاجم شهادة موقعة من نفس المرجع المصدق (وهو ما يحدث غالباً في عمليات النشر الداخلية مع البنية التحتية للمفاتيح العامة للمؤسسة)، فيمكنه الانضمام إلى المجموعة.

بالإضافة إلى ذلك، لا تستخدم العديد من عمليات نشر Galera التحقق المتبادل من الشهادات (TLS المتبادل). أنها تمكن TLS للتشفير ولكن ليس للمصادقة.

الحل: wsrep_allow_list

منذ MariaDB 10.10، يوفر المتغير `wsrep_allow_list` آلية قائمة IP البيضاء للعقد المسموح لها بالانضمام إلى المجموعة:

```
[mysqld]
wsrep_allow_list = 10.0.1.10,10.0.1.11,10.0.1.12
```

فقط العقد التي يوجد عنوان IP الخاص بها في القائمة يمكنها الانضمام إلى المجموعة. سيتم رفض العقدة ذات عنوان IP غير المُدرج، حتى لو كانت تحتوي على بيانات اعتماد SST وشهادات TLS الصحيحة.

إنها بسيطة وفعالة، وهي خط الدفاع الأول الذي يجب أن تمتلكه أي مجموعة Galera.

الدفاع في العمق

لا يعتمد أمان مجموعة Galera على آلية واحدة. هنا هو الدفاع في نهج العمق:

1. wsrep_allow_list — تصفية الشبكة

```
wsrep_allow_list = 10.0.1.10,10.0.1.11,10.0.1.12
```

تقييد عناوين IP المسموح لها بالانضمام إلى المجموعة.

2. TLS المتبادل — مصادقة العقدة

```
wsrep_provider_options = "socket.ssl=yes;socket.ssl_key=/etc/mysql/ssl/server-
key.pem;socket.ssl_cert=/etc/mysql/ssl/server-cert.pem;socket.ssl_ca=/etc/mysql/ssl/ca.pem"
```

يجب أن تقدم كل عقدة شهادة موقعة من قبل المجموعة CA. لا توجد شهادة صالحة = لا يوجد اتصال.

3. شبكة معزولة - تجزئة

يجب أن يتم تداول حركة مرور Galera (المنافذ 4567، 4568، 4444) على شبكة مخصصة، معزولة عن شبكة التطبيق وشبكة الإدارة. يوصى باستخدام شبكة VLAN مخصصة أو شبكة متراكبة (WireGuard، IPsec).

4. جدار الحماية — تصفية المنافذ

```
# iptables : n'autoriser que les IPs du cluster sur les ports Galera
iptables -A INPUT -p tcp -s 10.0.1.10 --dport 4567 -j ACCEPT
iptables -A INPUT -p tcp -s 10.0.1.11 --dport 4567 -j ACCEPT
```

```
iptables -A INPUT -p tcp -s 10.0.1.12 --dport 4567 -j ACCEPT
iptables -A INPUT -p tcp --dport 4567 -j DROP
```

5. بيانات اعتماد SST مشفرة

لا تقم مطلقاً بتخزين كلمات مرور SST بنص واضح في ملفات التكوين. استخدم المديرين السريين (Vault، AWS Secrets Manager) أو على الأقل تشفير ملفات التكوين.

تدقيق مجموعتك

تحقق من حالة الأمان لمجموعة Galera الخاصة بك الآن:

```
-- Vérifier si wsrep_allow_list est configuré
SHOW VARIABLES LIKE 'wsrep_allow_list';

-- Vérifier l'état TLS de Galera
SHOW STATUS LIKE 'wsrep_connected';
SHOW VARIABLES LIKE 'wsrep_provider_options';

-- Lister les nœuds actuels du cluster
SELECT * FROM information_schema.WSREP_MEMBERSHIP;
```

إذا كان `wsrep_allow_list` فارغاً، فإن مجموعتك معرضة للخطر. قم بإعداده على الفور.

الخلاصة

تعد ثغرة Galera SST بمثابة ناقل هجوم تم الاستهانة به. يمكن للعقدة المارقة الحصول على نسخة كاملة من قاعدة البيانات الخاصة بك ببساطة عن طريق الانضمام إلى المجموعة. الحل بسيط: `wsrep_allow_list` + TLS متبادل + شبكة معزولة + جدار حماية.

35% من تسرب البيانات عبارة عن تهديدات داخلية. هل مجموعتك Galera محمية؟

تم نشر هذه المقالة في الأصل على متوسط.