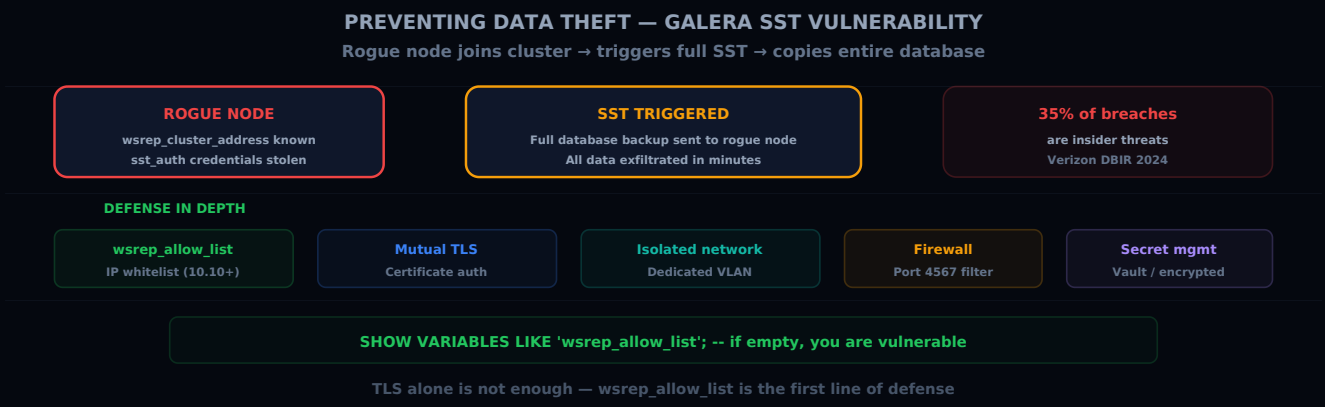
Zapobieganie kradzieży danych: edycja Galera

Sylvain ARBAUDIE · March 12, 2025

GALERA MARIADB SECURITY SST



Scenariusz koszmarny

Wyobraź sobie: atakujący konfiguruje serwer MariaDB z odpowiednimi parametrami wsrep, zna adres klastra Galera i hasło SST. Dołącza do klastra. Galera wykrywa nowy węzeł bez danych i wyzwala **State Snapshot Transfer (SST)** — pełny transfer wszystkich danych klastra do węzła atakującego.

W kilka minut (lub godzin, zależnie od rozmiaru bazy) atakujący posiada integralną kopię Twojej bazy danych. Bez iniekcji SQL, bez eksploitacji podatności aplikacyjnej. Tylko dołączenie do klastra z odpowiednimi danymi uwierzytelniającymi.

To nie science fiction. Według raportu Verizon 2024 o wyciekach danych, **35% naruszeń danych dotyczy zagrożeń wewnętrznych** — pracowników, podwykonawców lub osób z legalnym dostępem do infrastruktury.

Jak działa SST

State Snapshot Transfer to mechanizm, przez który Galera inicjalizuje nowy węzeł. Gdy węzeł dołącza do klastra bez danych (lub z danymi zbyt starymi dla przyrostowego IST), klaster wyzwala SST:

1. Wybierany jest węzeł donora (istniejący członek klastra)

2. Donor wykonuje pełną kopię zapasową (przez mariabackup, rsync lub mysqldump)
3. Kopia jest wysyłana do dołączającego węzła przez sieć
4. Dołączający węzeł przywraca kopię i dołącza do klastra

Problem: **domyślnie każdy węzeł z poprawnymi informacjami o klastrze może wywołać SST**. Nie ma białej listy, nie ma weryfikacji tożsamości dołączającego węzła.

Minimalna konfiguracja do ataku

Czego potrzebuje atakujący:

```
[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
```

Trzy informacje: adres klastra, metoda SST i dane uwierzytelniające SST. W wielu organizacjach te informacje są przechowywane w nieszyfrowanych plikach konfiguracyjnych, jawnych playbookach Ansible lub prywatnych repozytoriach Git.

Dlaczego TLS nie wystarczy

"Ale używamy TLS dla ruchu Galera!" — to częsta obiekcja. I jest niewystarczająca.

TLS szyfruje ruch między węzłami, ale nie weryfikuje koniecznie tożsamości dołączającego węzła. Nawet z TLS, jeśli atakujący posiada certyfikat podpisany przez to samo CA (co jest częste we wdrożeniach wewnętrznych z korporacyjną PKI), może dołączyć do klastra.

Ponadto wiele wdrożeń Galera nie używa wzajemnej weryfikacji certyfikatów (mutual TLS). Aktywują TLS dla szyfrowania, ale nie dla uwierzytelniania.

Rozwiązanie: wsrep_allow_list

Od MariaDB 10.10 zmienna `wsrep_allow_list` oferuje mechanizm białej listy IP dla węzłów upoważnionych do dołączenia do klastra:

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

Tylko węzły, których adres IP figuruje na liście, mogą dołączyć do klastra. Węzeł z IP spoza listy zostanie odrzucony, nawet jeśli posiada poprawne dane uwierzytelniające SST i właściwe certyfikaty TLS.

To proste, skuteczne i jest pierwszą linią obrony, którą każdy klaster Galera powinien mieć.

Obrona w głąb

Bezpieczeństwo klastra Galera nie opiera się na jednym mechanizmie. Oto podejście obrony w głąb:

1. wsrep_allow_list — Filtrowanie sieciowe

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

Ograniczenie IP upoważnionych do dołączenia do klastra.

2. Wzajemne TLS — Uwierzytelnianie węzłów

```
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"
```

Każdy węzeł musi przedstawić certyfikat podpisany przez CA klastra. Brak ważnego certyfikatu = brak połączenia.

3. Izolowana sieć — Segmentacja

Ruch Galera (porty 4567, 4568, 4444) powinien przechodzić przez dedykowaną sieć, odizolowaną od sieci aplikacyjnej i sieci zarządzania. Zalecany jest dedykowany VLAN lub sieć nakładkowa (WireGuard, IPsec).

4. Firewall — Filtrowanie portów

```
# iptables: zezwolenie tylko IP klastra na portach 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. Zaszyfrowane dane uwierzytelniające SST

Nigdy nie przechowuj haseł SST w tekście jawnym w plikach konfiguracyjnych. Używaj menedżerów sekretów (Vault, AWS Secrets Manager) lub minimum szyfrowania plików konfiguracyjnych.

Audyt klastra

Sprawdź natychmiast stan bezpieczeństwa swojego klastra Galera:

```
-- Sprawdzenie, czy wsrep_allow_list jest skonfigurowany
SHOW VARIABLES LIKE 'wsrep_allow_list';

-- Sprawdzenie stanu TLS Galera
SHOW STATUS LIKE 'wsrep_connected';
SHOW VARIABLES LIKE 'wsrep_provider_options';

-- Lista aktualnych węzłów klastra
SELECT * FROM information_schema.WSREP_MEMBERSHIP;
```

Jeśli `wsrep_allow_list` jest pusty, Twój klaster jest podatny. Skonfiguruj go natychmiast.

Podsumowanie

Podatność SST w Galera to niedoceniany wektor ataku. Nieautoryzowany węzeł może uzyskać pełną kopię Twojej bazy danych, po prostu dołączając do klastra. Rozwiązanie jest proste: `wsrep_allow_list` + wzajemne TLS + izolowana sieć + firewall.

35% wycieków danych to zagrożenia wewnętrzne. Czy Twój klaster Galera jest chroniony?

Ten artykuł został pierwotnie opublikowany na Medium.