Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 23 janvier 2017
N° CERTFR-2017-ACT-004

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-004

1 - Contrôle d'accès ligne par ligne dans les bases de données

Le contrôle d'accès au sein d'un système de gestion de base de données relationnelles (SGBDR) est traditionnellement mis en place avec la commande GRANT, qui fait partie du standard SQL. Par exemple on accorde le droit d'accès en lecture à l'utilisateur 'demo' pour la table 'correlation_alerts' avec l'expression suivante :

```
GRANT SELECT ON correlation_alerts TO demo;
```

On peut attribuer différents privilèges (SELECT, INSERT, EXECUTE, etc) à un utilisateur pour n'importe quel objet de la base de données, si on en est propriétaire. La granularité de ce système de droits est donc celui de l'objet : table, index, fonction, etc.

Pour un certain nombre de cas d'utilisation, cette granularité n'est pas assez fine. Pour une table donnée, on aimerait pouvoir établir un contrôle d'accès au niveau de la ligne, voire de la cellule. Nous nous intéressons ici au contrôle d'accès qui s'applique à chaque ligne d'une table donnée, nommé Row Level Security. Cette fonctionnalité est disponible pour plusieurs SGBDRs dont Oracle, Microsoft SQL Server, et PostgreSQL depuis la version 9.5.

Row Level Security permet de restreindre l'accès à une table à un sous-ensemble de celle-ci. Pour cela le propriétaire de la table définit une ou plusieurs règles ; chaque règle est associée à un ou plusieurs utilisateur(s), un type de requête (SELECT, INSERT, UPDATE ou DELETE), et un prédicat qui sera évalué sur chacune des lignes.

Exemple avec PostgreSQL

La fonctionnalité doit être activée explicitement pour chaque table :

```
ALTER TABLE table_name ENABLE ROW LEVEL SECURITY;
```

On définit ensuite une règle de sécurité. Si par exemple on a une table 'correlation_alerts' correspondant aux alertes de corrélation d'un SIEM, et que l'on souhaite interdire l'accès aux alertes dont la classification commence par 'APT' à l'utilisateur 'demo' :

```
CREATE POLICY apt_alerts ON correlation_alerts
       FOR SELECT USING (current_user != 'demo' OR classif NOT LIKE 'APT%');
```

Il est possible d'écrire des règles plus complexes, au prix d'un impact sur les performances :

```
CREATE POLICY apt_alerts ON correlation_alerts FOR SELECT
USING (classif NOT LIKE 'APT%' OR
      (SELECT permission FROM user_perm WHERE user = current_user) = 'VIEW_APT_ALERTS');
```

Du point de vue de l'utilisateur, tout se passe comme si les lignes auxquelles il n'a pas accès n'existent pas : si certaines lignes ne lui sont pas retournées, rien ne lui indique. On se réfèrera à la documentation pour plus de détails, notamment les possibles fuites d'information, et comment y remédier.

Documentation

- http://docs.postgresqlfr.org/current/ddl-rowsecurity.html
- https://www.postgresql.org/docs/current/static/ddl-rowsecurity.html (version originale de [1])
- https://msdn.microsoft.com/en-us/library/cc966395.apx

2 - Rappel des avis émis

Dans la période du 16 au 22 janvier 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-013 : Multiples vulnérabilités dans ISC BIND
- CERTFR-2017-AVI-014 : Multiples vulnérabilités dans Moodle
- CERTFR-2017-AVI-015 : Multiples vulnérabilités dans Citrix Provisionning Services
- CERTFR-2017-AVI-016 : Multiples vulnérabilités dans le noyau Linux de SUSE
- CERTFR-2017-AVI-017 : Multiples vulnérabilités dans Oracle Java SE
- CERTFR-2017-AVI-018 : Multiples vulnérabilités dans Oracle MySQL
- CERTFR-2017-AVI-019 : Multiples vulnérabilités dans Oracle Linux and Virtualization
- CERTFR-2017-AVI-020 : Multiples vulnérabilités dans Oracle Database Server
- CERTFR-2017-AVI-021 : Multiples vulnérabilités dans Oracle Sun Systems Products Suite
- CERTFR-2017-AVI-022 : Multiples vulnérabilités dans Juniper Network and Security Manager
- CERTFR-2017-AVI-023 : Multiples vulnérabilités dans Cisco WebEx Meetings Server et Center
- CERTFR-2017-AVI-024 : Vulnérabilité dans SCADA Schneider homeLYnk Controller

Gestion détaillée du document

23 janvier 2017 version initiale.