VA2108 Rule - Customer Facing Error Message

Last updated by | Soma Jagadeesh | Jul 5, 2021 at 1:09 PM PDT

Contents

- Issue
- Investigation/Analysis
- Mitigation
- RCA Template (optional)
- More Information (optional)
- Public Doc Reference (optional)
- Internal Reference (optional)
- Root Cause Classification

Issue

VA2108 Rule, If the dbo user is not the baseline, we are suggesting for the customers to remove the dbo user from the db_owner role

Investigation/Analysis

Query that was causing "false" alert:

```
SELECT user_name(sr.member_principal_id) as [Principal]
    ,user_name(sr.role_principal_id) as [Role]
    ,type_desc as [Principal Type]
    ,authentication_type_desc as [Authentication Type]
FROM sys.database_role_members AS sr
INNER JOIN sys.database_principals AS sp ON sp.principal_id = sr.member_principal_id
WHERE sr.role_principal_id IN (user_id('bulkadmin'),
                               user_id('db_accessadmin'),
                               user_id('db_securityadmin'),
                               user_id('db_ddladmin'),
                               user_id('db_backupoperator'),
                               user_id('db_owner'))
```

The correct query should be:

```
 SELECT user_name(sr.member_principal_id) AS [Principal]
    ,user_name(sr.role_principal_id) AS [Role]
    ,type_desc AS [Principal Type]
    ,authentication_type_desc AS [Authentication Type]
FROM sys.database_role_members AS sr
INNER JOIN sys.database_principals AS sp ON sp.principal_id = sr.member_principal_id
WHERE sr.role_principal_id IN (
        user_id('bulkadmin'),
        user_id('db_accessadmin'),
        user_id('db_securityadmin'),
        user_id('db_ddladmin'),
        user_id('db_backupoperator'))
    OR (sr.role_principal_id = user_id('db_owner')
        AND sr.member_principal_id <> user_id('dbo'))
```

Mitigation

A fix will be deployed.

ICM 247572018

RCA Template (optional)

We have identified this issue and received feedback on this VA 2108 Rule and customer challenges.

Status: A fix is being deployed. See ICM 247572018.

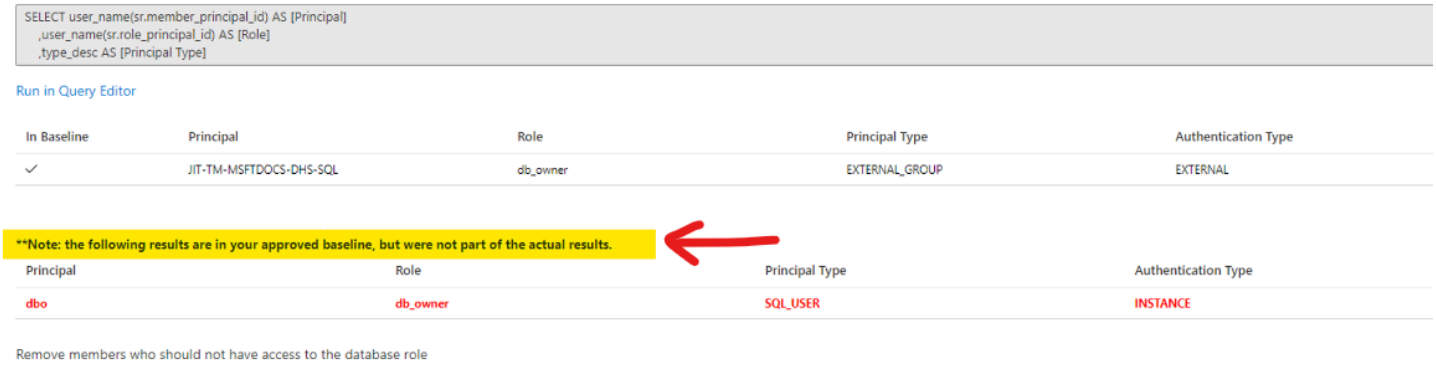
More Information (optional)

Information the VA should not be interested on the dbo user Users(database_user, sid) AS (SELECT principal_name ,sid FROM UsersAndRoles WHERE type IN ('S' ,'X' ,'E' ,'G') AND principal_name != 'dbo')

VA2108 has been updated to exclude the dbo, not deprecated.

The deployment is in progress and has not been fully deployed WW yet.

In the attached “Figure 2” it can be seen that the dbo is no longer returned as a result but is part of the baseline.



Customer needs to clear the baseline and set it again.

Public Doc Reference (optional)

Internal Reference (optional)

For example, on VA2130 we are already skipping the dbo user.

- ETA for fix to be deployed WW by the end of June.
- Customers who have set up a baseline on this rule will be notified by email before change is being deployed

Root Cause Classification

/Vulnerability Assessment/VA Rules

How good have you found this content?