**به نام خدا**

**پیکربندی امن**

# پایگاه داده MS SQL Server 2012

**مرکز مدیریت راهبردی افتا**

SCDB-MS-SQL-SER -2012

فروردین ۹۶

نسخه ۱,۰

# فهرست

# پیش‌گفتار

مرکز مدیریت راهبردی افتا[1] به منظور ساماندهی امنیت تجهیزات در حوزه فاوا[2]، پروژه «پیکربندی امن محصولات IT در کشور» را آغاز نموده است. یکی از گام‌های اساسی در این پروژه ارائه چک‌لیست و راهنمای پیکربندی امن برای محصولات IT می‌باشد. ارائه چک‌لیست برای محصولات داخلی بر عهده تولیدکننده محصول می‌باشد. تولید کننده ملزم است، چک‌لیست خود را در غالب ارائه شده از سمت مرکز افتا ارائه دهد. چک‌لیست‌های ارائه شده، توسط مرکز افتا مورد ارزیابی قرار گرفته و منتشر می‌گردد. سازمان‌های دولتی ملزم به استفاده از چک لیست‌های مذکور برای محصولات در حال استفاده خود هستند. همچنین سازمان‌های دولتی موظفند قبل از استفاده از محصولات IT، آن‌را مطابق چک‌لیست امنیتی مورد تایید مرکز افتا پیکربندی نمایند.

توجه به این نکته حائز اهمیت می‌باشد که چک‌لیست‌های ارائه شده، یک امنیت سطح پایه برای محصول ایجاد می‌نماید و سازمان‌ها ملزم هستند که برای رسیدن به سطح امنیت مورد نیاز خود، پس از اجرای مدیریت ریسک[3]، الزامات دیگری را نیز به این تنظیمات اضافه و مستند نمایند.

[1] امنیت فضای تولید و تبادل اطلاعات
[2] فناوری اطلاعات و ارتباطات
[3] Risk management

## مقدمه

این سند، راهنمایی برای پیکربندی امن Microsoft SQL Server 2012 است. در این سند مقادیر و تنظیمات مناسب برای امن سازی سیاست‌ها و پیکربندهای محصول یاد شده ارائه شده است. مدیر سامانه با استفاده از این سند می‌تواند تنظیمات ارائه شده را پیاده سازی نماید.

این سند توسط شرکت "توسعه‌گران فناوری اطلاعات و آموزش آرمان داده پویان" و به درخواست و تحت نظارت مرکز مدیریت راهبردی افتا تهیه گردیده است و از تلاش کارشناسان آن شرکت صمیمانه قدردانی می‌گردد. مرکز مدیریت راهبردی افتا ضمن استقبال از نظرات کارشناسان و متخصصان این حوزه برای غنای بیشتر این سند و دیگر اسناد مقاوم سازی، آمادگی دریافت پیشنهادات سازنده از طریق آدرس پست الکترونیکی Hardening@aftasec.ir را اعلام می‌دارد.

در ادامه، تنظیمات مورد نیاز برای پیکربندی امن Microsoft SQL Server 2012 آمده است. در این سند هر تنظیم با یک نام لاتین و شماره مختص آن آورده شده است. برای هر الزام دو بخش شرح اجمالی و نحوه پیاده‌سازی ارائه شده است. در بخش شرح اجمالی، توضیحی مختصر از ماهیت الزام بیان گردیده و در بخش نحوه پیاده‌سازی نیز، راهنمایی برای پیاده‌سازی الزام توسط مدیر سامانه ارائه شده است.

# تنظیمات

## ۱-**SCDB**: نصب و بروز رسانی

### ۱-۱-SCDB: بروز رسانی

#### شرح اجمالی

همواره از نصب آخرین و بروزترین وصله‌های امنیتی[۴] و بسته‌های سرویس[۵] اطمینان حاصل نمایید. وصله‌های امنیتی شامل بروز رسانی‌هایی هستند که ضعف‌های امنیتی را که مشخص شده‌اند، برطرف می‌کنند. بسته‌های سرویس نیز، هم شامل گروهی از وصله‌های امنیتی هستند و هم می‌توانند شامل وصله‌هایی به منظور بر طرف سازی برخی مشکلات کارایی باشند.

استفاده از آخرین نسخه نرم افزار به همراه تمام وصله‌های مناسب، می‌تواند در محدودسازی آسیب پذیری‌ها کمک کند.

#### نحوه پیاده سازی

جهت بررسی اینکه نگارش بسته سرویس مورد استفاده چیست، پرس و جو[۶] زیر را می‌توانیم اجرا کنیم:

```
SELECT SERVERPROPERTY('ProductLevel') as SP_installed,
SERVERPROPERTY('ProductVersion') as Version;
```

نتیجه شامل دو بخش اطلاعاتی است که بخش نخست نگارش بسته سرویس و بخش دوم نگارش دقیق ساخت[۷] نرم افزار را مشخص می‌سازد.

---

[۴] Security Patches
[۵] Service Pack
[۶] Query
[۷] Build Number

نسخه کنونی SQL Server و سطح وصله امنیتی خود را مشخص کنید و اطمینان حاصل کنید که از آخرین نسخه وصله‌های امنیتی استفاده کرده‌اید.

دریافت آخرین بروز رسانی‌ها هم می‌تواند به طور خودکار توسط Windows Update انجام شود و هم اینکه می‌توان بروز رسانی‌های مورد نظر را به صورت دستی از وبگاه مایکروسافت دریافت و نصب کرد.

نکته لازم اینکه، همواره یک محیط آزمایشی جهت نصب و بررسی وصله‌های امنیتی پیش بینی نمایید تا از صحت عملکرد آن‌ها مطمئن شوید.

بیشتر بروز رسانی‌های SQL Server را می‌توانید از نشانی زیر بدست آورید:

Hotfixes: http://blogs.msdn.com/b/sqlreleaseservices

Service Packs: https://support.microsoft.com/en-us/kb/2755533

۲-۱-SCDB: نصب بر روی یک سرویس دهنده انحصاری و تک کاربرد صورت گیرد.

شرح اجمالی

توصیه می‌گردد که SQL Server بر روی یک سرور اختصاصی نصب شود. در این حالت انعطاف پذیری بیشتری جهت اعمال سیاست‌های امنیتی وجود دارد. همچنین امکان ایجاد دسترسی‌های خاص از سمت سرور و یا به سمت سرور، و یا از طریق پروتکل خاص، با سهولت و اطمینان بیشتری امکان‌پذیر است. این سطح از دسترسی روی سرور می‌تواند انتقال از یک پایگاه داده به نگارش دیگر و یا انتقال بر روی زیر ساخت دیگری را آسان‌تر نماید.

همچنین پایگاه داده تحت تاثیر آسیب پذیری‌ها و ضعف‌های امنیتی سایر برنامه‌ها و سرویس‌ها قرار نمی‌گیرد.

نحوه پیاده سازی

اطمینان حاصل شود بر روی سیستم عامل سرویس دهنده پایگاه داده، هیچ نقش دیگری فعال نیست.، یا هیچ ابزار متفاوتی نصب نشده است. این مورد از طریق بررسی سرویس‌های موجود در کنسول services.msc و همچنین برنامه‌های نصب شده که در کنسول appwiz.cpl نمایش داده می‌شوند، می‌تواند انجام شود. برای دسترسی به کنسول‌های نام برده شده، نام کنسول را در قسمت Run ویندوز وارد و اجرا نمایید.

کنسول Server Manager نیز میتواند برای این موضوع مورد استفاده قرار گیرد. به منظور دسترسی به این کنسول، در Run ویندوز عبارت ServerManager را وارد و اجرا نمایید.

## ۲-**SCDB**: کاهش سطح آسیب پذیری

### ۱-۲-SCDB: گزینه Ad Hoc Distributed Queries را غیر فعال کنید.

شرح اجمالی

این گزینه، اجازه اجرای پرس و جو و یا اجرای دستورات بر روی یک پایگاه داده خارجی را به کاربر می‌دهد و در نتیجه باید غیر فعال گردد.

این گزینه می‌تواند به منظور دسترسی از راه دور و بهره برداری از آسیب پذیری‌های پایگاه داده و در نهایت اجرای کدها و توابع مخرب بر روی آن‌ها مورد استفاده قرار گیرد.

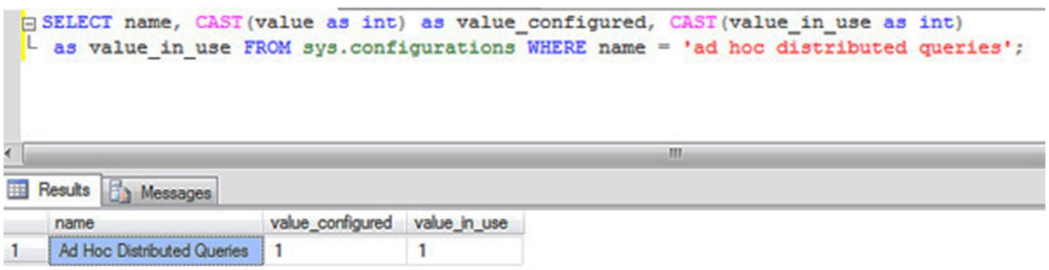
نحوه پیاده سازی

جهت اطلاع از وضعیت این گزینه، پرس و جوی زیر را اجرا کنید:

```
SELECT name, CAST(value as int) as value_configured, CAST(value_in_use as int) as value_in_use FROM sys.configurations WHERE name = 'ad hoc distributed queries';
```

هر دو شناسه بازگشتی حاصل از این پرس و جو باید معادل 0 باشند.

شکل زیر نشان دهنده حالتی می‌باشند که در آن این خصیصه فعال می‌باشد:




در صورت فعال بودن، با اجرای فرمان زیر این خصیصه غیر فعال می‌شود:

```
EXECUTE sp_configure 'show advanced options', 1;
RECONFIGURE;
EXECUTE sp_configure 'Ad Hoc Distributed Queries', 0;
RECONFIGURE;
EXECUTE sp_configure 'show advanced options', 0;
RECONFIGURE;
```

با اجرای صحیح فرمان بالا، نتیجه‌ای به صورت زیر باز خواهد گشت:

```
Configuration option 'show advanced options' changed from 1 to 1.
Run the RECONFIGURE statement to install.
Configuration option 'Ad Hoc Distributed Queries' changed from 1 to 0.
Run the RECONFIGURE statement to install.
Configuration option 'show advanced options' changed from 1 to 0.
Run the RECONFIGURE statement to install.
```

## ۲-۲-SCDB : گزینه CLR Enabled[۸] را غیر فعال کنید.

### شرح اجمالی

CLR، در اصل هسته مرکزی Net Framework. است که امکان اجرای کدهای اجرایی را می‌دهد. این محیط توانایی اجرا و مدیریت امکانات قابل توجهی از سیستم عامل را دارد. توسط CLR که در SQL Server میزبانی می‌شود، امکان تعریف و نوشتن رویه‌های ذخیره شده، توابع، Triggerها و سایر موارد مشابه وجود دارد. استفاده از این محیط و توسعه امکانات در آن افزایش کارایی را در اجرای برنامه‌ها به دنبال دارد.

فعال بودن این امکان، سطح حملات قابل تعریف بر روی سرور و نیز ریسک اجرای کدهای مخرب را که به صورت عمدی یا غیر عمدی به سرور ارجاع می‌شوند را افزایش می‌دهد.

### نحوه پیاده سازی

از طریق اجرای فرمان زیر وضعیت این گزینه بررسی می‌شود:

```
SELECT name, CAST(value as int) as value_configured,
CAST(value_in_use as int) as value_in_use FROM sys.configurations
WHERE name = 'clr enabled';
```

هر دو مقدار بازگشتی از این پرس وجو باید مقدار 0 باشد.

در صورت فعال بودن، فرمان زیر را جهت غیر فعال کردن این تنظیم اجرا نمایید:

```
EXECUTE sp_configure 'clr enabled', 0; RECONFIGURE;
```

[۸] Common Language Runtime

## ۳-۲-SCDB : Cross DB Ownership Chaining را غیرفعال سازید.

### شرح اجمالی

این امکان، دسترسی به پایگاه داده‌های مختلف تحت یک مالکیت را در سطح یک سرویس دهنده یا یک Instance فراهم می‌سازد.

این امکان باعث می‌شود وقتی یک کاربر دارای نقش db_owner بر روی یک پایگاه داده باشد، امکان ورود و دسترسی روی سایر پایگاه داده را نیز داشته باشد. این موضوع باعث دسترسی‌های غیر ضروری و نوعی افشای اطلاعات می‌گردد. در صورتیکه نیاز به این دسترسی بر روی پایگاه داده وجود داشته باشد، این تنظیم تنها در سطح آن پایگاه داده و از طریق فرمان زیر اعمال شود:

```
ALTER DATABASE <dbname> SET DB_CHAINING ON
```

### نحوه پیاده سازی

جهت مشخص شدن وضعیت این تنظیم، پرس و جوی زیر را اجرا می‌کنیم:

```
SELECT name, CAST(value as int) as value_configured, CAST(value_in_use
as int) as value_in_use FROM sys.configurations WHERE name = 'Cross db
ownership chaining';
```

هر دو مقدار بازگشتی حاصل از این پرس و جو باید مقدار 0 باشد.

در صورت فعال بودن، فرمان زیر را اجرا می‌کنیم:

```
EXECUTE sp_configure 'Cross db ownership chaining', 0; RECONFIGURE;
```

## SCDB-۲-۴ : Database Mail XPs را غیرفعال سازید.

### شرح اجمالی

این گزینه تولید و انتقال رایانامه از سمت SQL Server را کنترل می‌نماید. این امکان توسط یک SMTP Server امکان پذیر می‌باشد و تنظیمات آن نیز در MSDB نگهداری می‌شود. تنها کاربران دارای نقش‌های SysAdmin و DatabaseMailUserRole بصورت پیش فرض دسترسی ارسال رایانامه را دارند.

با غیر فعال سازی این گزینه، امکان ایجاد حملات DoS[۹] به سرور از طریق ارتباط با خارج از سرور، کاهش می‌یابد.

### نحوه پیاده سازی

جهت مشخص شدن وضعیت این تنظیم، پرس وجوی زیر را اجرا می‌کنیم:

```
SELECT name, CAST(value as int) as value_configured, CAST(value_in_use
as int) as value_in_use FROM sys.configurations WHERE name = 'Database
Mail XPs';
```

هر دو مقدار بازگشتی حاصل از این پرس و جو باید مقدار 0 باشد.

در صورت فعال بودن، فرمان زیر را اجرا می‌کنیم:

```
EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE;
EXECUTE sp_configure 'Database Mail XPs', 0; RECONFIGURE;
```

[۹] Denial of Service

## SCDB-۲-۵ : Ole Automation Procedures را غیرفعال سازید.

### شرح اجمالی

این گزینه، امکان اجرای برنامه‌ها، فرمان‌ها و توابعی در خارج از SQL Server را توسط رویه‌های ذخیره شده فراهم می‌سازد.

با فعال سازی این گزینه، سطح حملات به سرویس دهنده افزایش پیدا می‌کند و به کاربران امکان اجرای توابع در سطح امنیتی سرویس دهنده را خواهد داد.

### نحوه پیاده سازی

جهت مشخص شدن وضعیت این تنظیم، پرس و جوی زیر را اجرا می‌کنیم:

```
SELECT name, CAST(value as int) as value_configured, CAST(value_in_use
as int) as value_in_use FROM sys.configurations WHERE name = 'Ole
Automation Procedures';
```

هر دو مقدار بازگشتی حاصل از این پرس و جو باید مقدار 0 باشد.

در صورت فعال بودن، فرمان زیر را اجرا می‌کنیم:

```
EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE;
EXECUTE sp_configure ' Ole Automation Procedures', 0; RECONFIGURE;
EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;
```

## ۶-۲-SCDB : Remote Access را غیرفعال سازید.

### شرح اجمالی

با فعال سازی این گزینه، امکان اجرای رویه‌های ذخیره شده محلی بر روی سرورهای دیگر و یا اجرای رویه‌های ذخیره شده سرورهای دیگر روی سرور محلی وجود خواهد داشت.

این قابلیت می‌تواند باعث سوءاستفاده و راه اندازی یک حمله DoS بر روی یک سرور دیگر شود. برای این منظور هنگامی که این قابلیت بر روی یک سرور فعال می‌باشد می‌توان پرس و جوهای سنگینی را بر روی آن سرور ارسال و اجرا نمود.

### نحوه پیاده سازی

جهت مشخص شدن وضعیت این تنظیم، پرس وجوی زیر را اجرا می‌کنیم:

```
SELECT name, CAST(value as int) as value_configured, CAST(value_in_use
as int)as value_in_use FROM sys.configurations WHERE name = 'Remote
access';
```

هر دو مقدار بازگشتی حاصل از این پرس و جو باید مقدار 0 باشد.

در صورت فعال بودن، فرمان زیر را اجرا می‌کنیم:

```
EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE;
EXECUTE sp_configure 'Remote access', 0; RECONFIGURE;
EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;
```

SCDB-۲-۷: Remote Admin Connection را غیرفعال سازید.

## شرح اجمالی

این تنظیم مشخص می‌نماید که کدام کاربر می‌تواند از دسترسی انحصاری مدیریت[۱۰] یا DAC استفاده کند. دسترسی DAC اجازه نوعی دسترسی مدیریتی را می‌دهد که امکان اجرای توابع تشخیصی از سرور درحال اجرا، اجرای دستورات T-SQL و یا بررسی اشکالات موجود در سرور بانک اطلاعاتی را دارد. حتی در وضعیتی که سرور Lockو یا در وضعیت غیر معمولی باشد که به بانک‌های اطلاعاتی پاسخگو نباشد.

در وضعیت Cluster مدیر سیستم ممکن است بصورت واقعی بر روی یک سرور وصل نشود. در این حالت دسترسی نوعی از دسترسی از راه دور است، بنابر این باید مقدار این متغیر در تنظیمات '1' یا فعال باشد. در غیر این صورت وضعیت غیر فعال یا '0' است.

## نحوه پیاده سازی

جهت مشخص شدن وضعیت این تنظیم، پرس و جوی زیر را اجرا می‌کنیم

```
SELECT name, CAST(value as int) as value_configured, CAST(value_in_use
as int) as value_in_use FROM sys.configurations WHERE name = 'Remote
admin connections' AND SERVERPROPERTY('IsClustered') = 0;
```

اگر هیچ مقداری باز نگردد، موجودیت بصورت Cluster تعریف شده و نباید تغییری اعمال گردد. اگر داده ای بازگشت، هر دو مقدار بازگشتی حاصل از این پرس و جو باید مقدار 0 باشد.

در صورت فعال بودن، فرمان زیر را اجرا می‌کنیم:

```
EXECUTE sp_configure 'Remote admin connections', 0; RECONFIGURE;
```

[۱۰] Dedicated Administrator Connection

SCDB-۲-۸: Scan for Startup Process را غیرفعال سازید.

## شرح اجمالی

این گزینه باعث اجرای خودکار رویه‌های ذخیره شده در SQL می‌شود.

اعمال این تنظیم، تهدید یک فرایند نفوذ را کاهش می‌دهد. به این صورت که از اجرای خودکار برخی رویه‌های ذخیره شده که در زمان بارگذاری سرویس اجرا می‌شوند، جلوگیری می‌نماید. در ضمن فرایند Replication به فعال بودن این امکان نیاز دارد و در صورت نیاز آن را بصورت اتوماتیک فعال می‌سازد.

## نحوه پیاده سازی

جهت مشخص شدن وضعیت این تنظیم، پرس و جوی زیر را اجرا می‌کنیم

```
SELECT name, CAST(value as int) as value_configured, CAST(value_in_use
as int) as value_in_use FROM sys.configurations WHERE name = 'Scan for
startup procs';
```

هر دو مقدار بازگشتی حاصل از این پرس و جو باید مقدار 0 باشد.

در صورت فعال بودن، فرمان زیر را اجرا می‌کنیم:

```
EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE;
EXECUTE sp_configure 'Scan for startup procs', 0; RECONFIGURE;
EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE
```

۹-۲-SCDB: مشخصه Trustworthy بانک اطلاعاتی را غیرفعال سازید.

## شرح اجمالی

این گزینه اجازه دسترسی اجزای بانک اطلاعاتی به اجزای سایر بانک‌های اطلاعاتی را تحت شرایط و موقعیت مشخصی ارائه می‌کند. با غیرفعال کردن این امکان، حفاظت در مقابل اسمبلی‌های CLR[۱۱] و یا رویه‌های توسعه یافته مهاجم ایجاد می‌گردد.

## نحوه پیاده سازی

جهت مشخص شدن لیست بانک‌های اطلاعاتی که در شرایط Trustworthy با این سرور هستند، پرس و جوی زیر را اجرا می‌کنیم

```
SELECT name FROM sys.databases WHERE is_trustworthy_on = 1
AND name != 'msdb' AND state = 0;
```

هر دو مقدار بازگشتی حاصل از این پرس و جو باید مقدار 0 باشد.

جهت اعمال عدم اعتماد برای بانک اطلاعاتی مشخص، فرمان زیر را اجرا می‌کنیم:

```
ALTER DATABASE <dbname> SET TRUSTWORTHY OFF;
```

[۱۱] Common Language Runtime

۱۰-۲-SCDB: پروتکل‌های غیر ضروری SQL Server را غیرفعال سازید.

شرح اجمالی

SQL Server پروتکل‌های Shared memory، Name Pipe، TCP/IP و VIA را پشتیبانی می‌نماید. با این حال، باید تنظیمات به نحوی اعمال شود که حداقل دسترسی‌ها مطابق با نیاز سازمانی ایجاد گردد.

استفاده از پروتکل‌های کمتر یا غیرفعال نمودن پروتکل‌های غیر ضروری، سطح حمله را کاهش می‌دهد و لایه ای از محافظت در مقابل تهدیدهای را ایجاد می‌نماید.

نحوه پیاده سازی

جهت مشخص شدن لیست پروتکل‌های مجاز، SQL Server Configuration Manager را باز می‌کنیم، به SQL Server Network Configuration می‌رویم و با مشاهده پروتکل‌ها، تنها موارد مورد نیاز را فعال می‌سازیم.

نکته: جهت اعمال تنظیمات ایجاد شده، می‌بایست سرویس بانک اطلاعاتی راه اندازی مجدد گردد.

SCDB-۲-۱۱ : SQL Server را با درگاه‌های متفاوت از درگاه‌های[۱۲] پیش فرض تنظیم کنید.

شرح اجمالی

در حالت معمول، SQL Server نصب شده بر روی سرور، درگاه شماره ۱۴۳۳ را جهت ارتباط پروتکل TCP/IP اختصاص می‌دهد. هرچند مدیر سیستم امکان تغییر این درگاه را دارد. با توجه به اینکه TCP:1443 تعریف مشخص و آشکاری است، این شماره درگاه باید تغییر نماید.

در نتیجه تعریف شماره درگاه غیر استاندارد، سطح محافظت بالاتری در مقابل تهدیدات اعمال می‌گردد.

نحوه پیاده سازی

در SQL Server Configuration Manager، بخش SQL Server Network Configuration، سپس Protocols، سپس TCP/IP را انتخاب می‌کنیم.

بر روی پنجره باز شده، در بخش IP Address، مجموعه و فهرست نشانی‌های IP را مشاهده می‌کنیم.

در بخش TCP Port مقدار 1433 را به مقدار دلخواه شماره درگاه تغییر می‌دهیم، و یا مقدار را خالی گذاشته و مقدار TCP Dynamic Port را صفر ثبت می‌کنیم تا امکان مقدار دهی متغیر برای شماره درگاه[۱۳] را فعال کنیم.

سرویس SQL Server را راه اندازی مجدد می‌نماییم تا تغییرات اعمال گردد.

به منظور بررسی صحت اجرای فرایند بالا، پنجره PowerShell را باز کرده و فرمان زیر را اجرا می‌کنیم، در حالت مناسب نباید هیچ سطر خروجی بازگردد.

```
PS C:\>netstat -ano | select-string 1433.+listening
```

[۱۲] Ports
[۱۳] Dynamic Port Assignment

با این تغییرات ممکن است در تنظیمات برخی برنامه‌ها و تجهیزات مانند دیواره‌های آتش[۱۴] تغییراتی اعمال گردد تا دسترسی‌های مورد نیاز برقرار گردد.

- اطمینان حاصل نمایید که پس از تغییر، کلیه برنامه‌های استفاده کننده از پایگاه داده نیز به درستی به فعالیت خود ادامه دهند. در صورت عدم اشراف بر برنامه های استفاده کننده از پایگاه داده، قبل از اعمال این تنظیم برنامه ریزی مناسب انجام دهید.

## SCDB-۲-۱۲ : مشخصه Hide instance بانک اطلاعاتی را فعال نمایید.

### شرح اجمالی

موجودیت[۱۵] سرورهای بانک اطلاعاتی SQL که به صورت غیر Cluster در محیطهای توسعه وجود دارند، باید بصورت مخفی تعیین شوند تا از معرفی توسط مرورگرهای سرورهای بانک اطلاعاتی SQL جلوگیری گردد.

در محیط‌های توسعه و تولید، این تنظیم باعث امنیت بیشتر سرور می‌گردد. البته در صورتیکه موجودیت بصورت Cluster تعریف شده باشد، این تنظیم موجب عدم عملکرد می‌گردد.

### نحوه پیاده سازی

در SQL Server Configuration Manager، بخش SQL Server Network Configuration، روی Protocol for server instance، کلیک راست نموده و مشخصات (property) را انتخاب می‌نماییم. در برگه مشخصات Flags، گزینه Yes را برای Hide Instance انتخاب نمایید.

[۱۴] Firewalls
[۱۵] Instance

SCDB-۲-۱۳ : شناسه کاربری sa را غیرفعال نمایید.

شرح اجمالی

شناسه کاربری sa به عنوان یک شناسه شناخته شده است که در اغلب سرورها با دسترسی بالا در گروه sysadmin وجود دارد. با غیر فعال نمودن این شناسه، احتمال اینکه یک مهاجم با استفاده از Brute-Force بتواند ایجاد تهدید نماید را حذف می‌نماییم.

نحوه پیاده سازی

با اجرای فرمان زیر می‌توان مشخص نمود که آیا شناسه sa فعال است یا خیر:

```
SELECT name, is_disabled FROM sys.server_principals WHERE sid = 0x01;
```

اگر مقدار بازگشتی برای متغیر ’is_disabled‘ معادل ۱ باشد، شناسه sa غیر فعال است.

جهت غیر فعال ساختن شناسه sa فرمان زیر را اجرا می‌نماییم:

```
ALTER LOGIN sa DISABLE;
```

اینکه برنامه‌ها یا اسکریپت‌ها از شناسه sa استفاده نمایند، راهبرد امنیتی مناسبی نیست، ولی در صورتیکه این اتفاق افتاده باشد، با اعمال تنظیم فوق، برنامه‌ها و اسکریپت‌های وابسته به کاربر sa از کار خواهند افتاد.

SCDB-۲-۱۴ : شناسه کاربری sa را تغییر نام[۱۶] دهید.

شرح اجمالی

شناسه کاربری sa به عنوان یک شناسه شناخته شده است که در اغلب سرورها با دسترسی بالا در گروه sysadmin وجود دارد. با تغییر نام این شناسه، قطعا استفاده از تکنیک Brute-Force برای کشف دسترسی سخت‌تر می‌گردد. چرا که نام کاربری نیز شناخته شده نیست.

نحوه پیاده سازی

با اجرای فرمان زیر می‌توان مشخص نمود که آیا شناسه sa تغییر نام یافته یا خیر.

```
SELECT name FROM sys.server_principals WHERE sid = 0x01;
```

اگر مقدار بازگشتی شناسه sa بود، شناسه هنوز تغییر نام نیافته است.

با اجرای فرمان زیر، شناسه sa را به نامی جدید تغییر نام می‌دهیم.

```
ALTER LOGIN sa WITH NAME = <نـام جدیـد>;
```

اینکه برنامه‌ها یا اسکریپت‌ها از شناسه sa استفاده نمایند، راهبرد امنیتی مناسبی نیست، ولی در صورتیکه این اتفاق افتاده باشد، با اعمال تنظیم فوق، برنامه‌ها و اسکریپت‌های وابسته به کاربر sa از کار خواهند افتاد.

[۱۶] Rename

SCDB-۲-۱۵ : در تنظیمات سرور امکان xp_cmdshell را غیرفعال نمایید.

شرح اجمالی

رویه xp_cmdshell به کاربران اعتبار سنجی[۱۷] شده SQL اجازه می‌دهد تا دستورات سیستم عامل را از طریق آن اجرا نمایند و نتیجه را در SQL Client باز گردانند.

xp_cmdshell بطور گسترده ای جهت دریافت اطلاعاتی از سیستم عامل میزبان بانک اطلاعاتی (خواندن یا نوشتن)، توسط مهاجمین مورد استفاده قرار می‌گیرد.

نحوه پیاده سازی

با اجرای فرمان زیر می‌توان مشخص نمود که رویه xp_cmdshell، فعال است یا خیر.

```
EXECUTE sp_configure 'show advanced options',1;
RECONFIGURE WITH OVERRIDE;
EXECUTE sp_configure 'xp_cmdshell';
```

اگر مقدار بازگشتی برای خروجی run_value صفر باشد، این رویه غیر فعال است.

با اجرای فرمان زیر، می‌توان مقدار این امکان را غیرفعال ساخت:

```
EXECUTE sp_configure 'show advanced options', 1;
RECONFIGURE;
EXECUTE sp_configure 'Xp_cmdshell', 0;
RECONFIGURE;
EXECUTE sp_configure 'show advanced options', 0;
RECONFIGURE;
```

[۱۷] Authenticated Users

## ۳-**SCDB**: احراز هویت[۱۸] و سنجش سطح دسترسی[۱۹]

### ۱-۳-SCDB: روش احراز هویت سرور را به احراز هویت ویندوز[۲۰] تغییر دهید.

شرح اجمالی

از اعتبارسنجی سمت سیستم عامل استفاده گردد. این روش در مقایسه با روش اعتبار سنجی در سطح بانک اطلاعاتی دارای مکانیزم‌های قدرتمندتری می‌باشد.

نحوه پیاده سازی

جهت بررسی نحوه اعتبار سنجی در بانک اطلاعاتی فرمان زیر را اجرا می‌نماییم:

```
xp_loginconfig 'login mode';
```

در صورتی که اعتبارسنجی توسط سیستم عامل صورت گیرد، خروجی و مقدار login mode، برابر با Windows NT Authentication است.

در صورتی که تنظیم مورد نظر نیاز به تغییر داشته باشد، به شرح زیر اقدام می‌شود:

۱- به Management Studio وارد می‌شویم.

۲- به موجودیت مورد نظر از سرور بانک اطلاعاتی متصل می‌شویم.

[۱۸] Authentication
[۱۹] Authorization
[۲۰] Windows Authentication

۳- از موجودیت، توسط کلیک راست، مشخصات را انتخاب می‌کنیم.

۴- از منوی سمت چپ، Security Mode را انتخاب می‌کنیم.

۵- در Server Authentication، روش اعتبارسنجی را به Windows Authentication mode تغییر می‌دهیم.

- از صحت عملکرد سیستم و برنامه‌ها پس از اعمال این تغییر اطمینان حاصل نمایید و در صورت اخلال در عملکرد، با بازگرداندن سیستم به حالت قبلی، برنامه‌ریزی مناسب برای اعمال آن انجام دهید.

## SCDB-۳-۲: محدود کردن دسترسی اتصال برای کاربران مهمان

دسترسی اتصال[۲۱] برای کاربران مهمان[۲۲] را بر روی تمام بانک‌های اطلاعاتی، بجز tempdb، msdb و master حذف نمایید.

### شرح اجمالی

حذف دسترسی کاربر مهمان، در ارتباط با بانک‌های اطلاعاتی سرویس دهنده. دسترسی به سرور بانک اطلاعاتی با دسترسی مهمان می‌تواند وجود داشته باشد، لکن دسترسی و مالکیت بانکهای اطلاعاتی نمی‌تواند در اختیار کاربر با این شناسه باشد. این تنظیم می‌تواند باعث اطمینان گردد که تنها راه دسترسی به بانک اطلاعاتی مشخص، تعریف کاربران مجاز است.

### نحوه پیاده سازی

جهت ارزیابی دسترسی کاربر مهمان به یک بانک اطلاعاتی خاص، فرمان زیر را اجرا می‌کنیم:

```
USE [database_name];
SELECT DB_NAME() AS DBName, dpr.name, dpe.permission_name
FROM sys.database_permissions dpe JOIN sys.database_principals dpr ON
dpe.grantee_principal_id=dpr.principal_id WHERE dpr.name='guest' AND
dpe.permission_name='CONNECT';
```

[۲۱] Connect
[۲۲] Guest Users

در صورتی که نتیجه‌ای بازگردد، دسترسی‌های مربوطه نیز اعلام می‌شوند.

جهت حذف دسترسی از فرمان زیر استفاده می‌کنیم.

```
USE [database_name];
REVOKE CONNECT FROM guest;
```

در صورتیکه این تنظیم اعمال گردد، دسترسی‌های مشخص باید جهت هر بانک اطلاعاتی تعریف گردد.

### SCDB-۳-۳ : کاربران اضافی و بدون ارتباط با بانک‌های اطلاعاتی را از روی سرور حذف نمایید.

شرح اجمالی

هرگونه تعریف شناسه‌های کاربری که مسئولیت متناسبی برای آن تعریف نشده باشد، اضافی است و باید از روی سرور حذف شود. وجود کاربرهای غیر ضروری روی سرور امکان سوءاستفاده از دسترسی‌ها را ایجاد می‌نماید.

نحوه پیاده سازی

جهت تشخیص کاربران اضافی، می‌توان پرس و جوی زیر را اجرا نمود:

```
EXEC sp_change_users_login @Action='Report';
```

جهت حذف کاربر اضافی، از فرمان زیر استفاده می‌کنیم:

```
DROP USER <username>;
```

## SCDB-۳-۴ : عدم استفاده از SQL authentication برای Contained Databases

### شرح اجمالی

خصیصه Contained Database، خصیصه‌ای است که در SQL Server 2012 به منظور ذخیره سازی تمامی اطلاعات مربوط به یک پایگاه داده در خودش اضافه شده است. نکته امنیتی که در این خصوص وجود دارد این است که قوانین مربوط به پیچیدگی گذرواژه در پایگاه داده‌ای که این خصیصه برای آن فعال شده است اعمال نمی‌شوند. از اینرو پیشنهاد می‌شود که از احراز هویت سیستم عامل بجای SQL Authentication برای این پایگاه‌های داده استفاده شود.

### نحوه پیاده سازی

به منظور یافتن شناسه‌های کاربری که از SQL Authentication در Contained Databaseها استفاده می‌کنند، فرمان زیر را برای هر پایگاه داده اجرا کنید:

```
SELECT name AS DBUser
FROM sys.database_principals
WHERE name NOT IN ('dbo','Information_Schema','sys','guest')
AND type IN ('U','S','G') AND authentication_type = 2;
GO
```

SCDB-۳-۵ : سرویس MSSQL نباید با شناسه کاربری مدیر سیستم یا در سطح مدیر سیستم اجرا شود.

## شرح اجمالی

شناسه کاربری که برای اجرای سرویس MSSQL به کار گرفته شده است نباید Administrator و یا به نوعی عضو گروه Administrators باشد. همچنین از شناسه کاربری LocalSystem نیز نباید برای اجرای این سرویس استفاده شود. این قبیل شناسه‌های کاربری دارای حق دسترسی‌هایی فراتر از نیاز سرویس MSSQL بر روی سیستم هستند.

## نحوه پیاده سازی

جهت تشخیص این موضوع از کنسول services.msc سرویس MSSQL را پیدا کرده و سپس شناسه کاربری که برای اجرای سرویس مشخص شده است را بیابید. در صورتیکه شناسه کاربری مشخص شده دارای حق دسترسی مدیر سیستم بود، لازم است تا یک شناسه کاربری با کمینه دسترسی به منظور اجرای سرویس MSSQL ایجاد شود و از آن به منظور اجرای سرویس استفاده شود.

به منظور اطمینان از اینکه شناسه کاربری ایجاد شده دارای دسترسی‌های لازم به منظور اجرای مناسب سرور و بارگذاری پایگاه‌های داده می‌باشد می‌توانید از SQL Server Configuration Manager Tool استفاده نمایید.

SCDB-۳-۶ : سرویس SQLAgent نباید با شناسه کاربری مدیر سیستم یا در سطح مدیر سیستم اجرا شود.

شرح اجمالی

شناسه کاربری که برای اجرای سرویس SQLAgent به کار گرفته شده است نباید Administrator و یا به نوعی عضو گروه Administrators باشد. همچنین از شناسه کاربری LocalSystem نیز نباید برای اجرای این سرویس استفاده شود. این قبیل شناسه‌های کاربری دارای حق دسترسی‌هایی فراتر از نیاز سرویس SQLAgent بر روی سیستم هستند.

نحوه پیاده سازی

جهت تشخیص این موضوع از کنسول services.msc سرویس SQLAgent را پیدا کرده و سپس شناسه کاربری که برای اجرای سرویس مشخص شده است را بیابید. در صورتیکه شناسه کاربری مشخص شده دارای حق دسترسی مدیر سیستم بود، لازم است تا یک شناسه کاربری با کمینه دسترسی به منظور اجرای سرویس SQLAgent ایجاد شود و از آن به منظور اجرای سرویس استفاده شود.

به منظور اطمینان از اینکه شناسه کاربری ایجاد شده دارای دسترسی‌های لازم به منظور اجرای مناسب سرور و بارگذاری پایگاه‌های داده می‌باشد می‌توانید از SQL Server Configuration Manager Tool استفاده نمایید.

SCDB-۳-۷ : سرویس Full-Text نباید با شناسه کاربری مدیر سیستم یا در سطح مدیر سیستم اجرا شود.

## شرح اجمالی

شناسه کاربری که برای اجرای سرویس Full-Text به کار گرفته شده است نباید Administrator و یا به نوعی عضو گروه Administrators باشد. همچنین از شناسه کاربری LocalSystem نیز نباید برای اجرای این سرویس استفاده شود. این قبیل شناسه‌های کاربری دارای حق دسترسی‌هایی فراتر از نیاز سرویس Full-Text بر روی سیستم هستند.

## نحوه پیاده سازی

جهت تشخیص این موضوع از کنسول services.msc سرویس Full-Text را پیدا کرده و سپس شناسه کاربری که برای اجرای سرویس مشخص شده است را بیابید. در صورتیکه شناسه کاربری مشخص شده دارای حق دسترسی مدیر سیستم بود، لازم است تا یک شناسه کاربری با کمینه دسترسی به منظور اجرای سرویس Full-Text ایجاد شود و از آن به منظور اجرای سرویس استفاده شود.

به منظور اطمینان از اینکه شناسه کاربری ایجاد شده دارای دسترسی‌های لازم به منظور اجرای مناسب سرور و بارگذاری پایگاه‌های داده می‌باشد می‌توانید از SQL Server Configuration Manager Tool استفاده نمایید.

## SCDB-۴ : قواعد گذرواژه

در این بخش توصیه‌هایی در خصوص قواعد گذرواژه ارائه می‌گردد.

SCDB-۴-۱ : مقدار شناسه MUST_CHANGE را برای تمام کاربرهای تایید شده فعال می‌کنیم.

شرح اجمالی

در صورتی که کاربر برای نخستین بار از login استفاده می‌کند، اخطار بروز رسانی گذرواژه برای وی نمایش داده می‌شود. الزام تغییر گذرواژه، از امکان دسترسی مدیر سیستم و یا هر کاربر، با گذرواژه اولیه جلوگیری می‌کند.

نحوه پیاده سازی

۱- به SQL Server Management Studio و Instance مورد نظر وصل می‌شویم.
۲- به بخش Logins می‌رویم ، بر روی کاربر مورد نظر کلیک راست کرده و وارد Properties می‌شویم.
۳- گزینه User must change password at next login باید انتخاب شده باشد.

با اجرای فرمان زیر برای هر شناسه کاربری امکان فعال سازی این مشخصه را داریم:

```
ALTER LOGIN login_name WITH PASSWORD = password_value MUST_CHANGE;
```

با این تنظیم، گزینه‌های CHECK_EXPIRATION و CHECK_POLICY باید فعال باشند.

## SCDB-۴-۲ : فعال سازی CHECK_EXPAIRATION برای تمام کاربرهای دارای نقش Sysadmin

### شرح اجمالی

این گزینه امکانی مانند قانون انقضای گذرواژه را برای شناسه‌های کاربری در بانک اطلاعاتی SQL Server ایجاد می‌کند.

اطمینان از اینکه شناسه‌های SQL کاملا با قواعد اعمال شده در سیستم عامل منطبق هستند و در نهایت گذرواژه‌های با دسترسی Sysadmin در بازه‌های زمانی مشخص تغییر می‌کند و این مورد باعث مقابله در برابر حملات Brute force می‌گردد.

### نحوه پیاده سازی

با اجرای فرمان زیر شناسه‌های کاربری عضو Sysadmin که دارای این تنظیم نیستند مشخص می‌گردند.

```
SELECT SQLLoginName = sp.name FROM sys.server_principals sp JOIN
sys.sql_logins AS sl ON sl.principal_id = sp.principal_id WHERE
sp.type_desc = 'SQL_LOGIN' AND sp.name in (SELECT name AS IsSysAdmin
FROM sys.server_principals p WHERE IS_SRVROLEMEMBER('sysadmin',name) =
1) AND sl.is_expiration_checked <> 1;
```

فرمان زیر را برای شناسه مورد نظر اجرا نمایید:

```
ALTER LOGIN [login_name] WITH CHECK_EXPIRATION = ON;
```

SCDB-۴-۳ : مقدار شناسه CHECK_POLICY را برای تمام کاربرهای تایید شده فعال نمایید.

شرح اجمالی

این مشخصه، قابلیت‌هایی شبیه به قوانین پیچیدگی گذرواژه در سیستم عامل را برای شناسه‌های کاربری SQL Server اعمال می‌نماید. اعمال این تنظیم که باعث می‌شود گذرواژه‌های ساده و یا شناسه‌های بدون گذرواژه در بانک اطلاعاتی تعریف نشوند و باعث ممانعت از افشای اطلاعات شناسه‌های کاربری در اثر حملات Brute force و یا سایر تهدیدات می‌گردد.

نحوه پیاده سازی

فرمان زیر را اجرا می‌کنیم:

```
SELECT SQLLoginName = sp.name, PasswordPolicyEnforced =
CAST(sl.is_policy_checked AS BIT) FROM sys.server_principals sp JOIN
sys.sql_logins AS sl ON sl.principal_id = sp.principal_id WHERE
sp.type_desc = 'SQL_LOGIN';
```

با این فرمان، شناسه‌های کاربری به همراه مشخصه مورد نظر لیست می‌گردند. در صورتیکه مشخصه PasswordPolicyEnforced معادل صفر باشد، مشخصه CHECK_POLICY باید فعال گردد.

با فرمان زیر، مشخصه بالا را برای شناسه کاربری مورد نظر فعال می‌کنیم:

```
ALTER LOGIN [login_name] WITH CHECK_POLICY = ON;
```

## SCDB-۵ : حسابرسی و رویدادنگاری

### SCDB-۵-۱ : مقداردهی مناسب برای بازنویسی فایل‌های رویداد خطا[۲۳]

شرح اجمالی

فایل‌های رویداد خطا برای بانک اطلاعاتی باید محافظت گردند و قبل از رونویسی[۲۴] از آنها پشتیبان گرفته شود.

فایل‌های رویداد، شامل اطلاعات مهمی در مورد فرایندهای اصلی سرور، و درخواست‌های ورود به سیستم هستند.

نحوه پیاده سازی

۱- به SQL Server Management Studio و Instance مورد نظر وصل می‌شویم.

۲- از Object explorer، به بخش Management رفته و با انتخاب SQL Server Logs، Configure را انتخاب می‌نماییم.

۳- حال گزینه‌ای که امکان انتخاب محدودیت تعداد فایل‌های رویداد، پیش از بازنویسی را می‌دهد ( Limit the number of error log files before they are recycled) انتخاب نموده و سپس تعداد را به ۱۲ تغییر می‌دهیم.

[۲۳] Error Log Files
[۲۴] Overwriting

۲-۵-SCDB : تنظیم Default Trace Enable را بر روی سرور بانک اطلاعاتی فعال کنید.

شرح اجمالی

این مشخصه، امکان ثبت و حسابرسی از رویدادهای فعالیت در سرور بانک اطلاعاتی شامل: ایجاد شناسه‌ها، ارتقای دسترسی‌ها و اجرای دستورات DBCC[۲۵] را ایجاد می‌نماید.

این امکان، باعث ایجاد داده‌ها و اطلاعات ارزشمندی در سطح امنیت بانک اطلاعاتی می‌گردد.

نحوه پیاده سازی

فرمان زیر را اجرا نمایید:

```
SELECT name, CAST(value as int) as value_configured, CAST(value in use
as int) as value_in_use FROM sys.configurations WHERE name = 'Default
trace enabled';
```

هر دو مقدار خروجی باید معادل ۱ باشند.

فرمان زیر را اجرا نمایید:

```
EXECUTE sp_configure 'show advanced options', 1;
RECONFIGURE;
EXECUTE sp_configure 'Default trace enabled', 1;
RECONFIGURE;
```

[۲۵] Database Console Command

SCDB-۵-۳ : امکان رویداد نگاری[۲۶] را برای ورودهای موفق و ناموفق تنظیم نمایید.

شرح اجمالی

حسابرسی از رویدادهای موفق و ناموفق جهت تلاش ورود و اتصال به بانک اطلاعاتی صورت می‌گیرد. اطلاعات حاصل شده، دارای ارزش زیادی جهت ارزیابی حملاتی است که برای حدس زدن گذرواژه و شناسه‌های سرور صورت می‌گیرد، همچنین اطلاعات ورودهای موفق به سرورها می‌تواند در تحقیقات بعدی جهت ارزیابی تغییرات اعمال شده مورد استفاده قرار گیرد.

نحوه پیاده سازی

فرمان زیر را اجرا کنید:

```
XP_loginconfig 'audit level';
```

در صورتی که مقدار خروجی all باشد، حسابرسی برای ورودهای موفق و ناموفق صورت می‌گیرد. در صورت فعال نبودن مراحل زیر را انجام دهید:

۱- SQL Server management Studio را باز کرده و به موجودیت مورد نظر متصل می‌شویم.

۲- با کلیک راست، مشخصات گرفته و به گزینه Security می‌رویم.

[۲۶] Log Auditing

۳- در قسمت Login Auditing ، گزینه : Both failed and success logins را انتخاب می‌کنیم.

۴- سرویس‌های SQL Server را راه اندازی مجدد می‌کنیم.

## SCDB-۶ : توسعه نرم افزار

### SCDB-۶-۱ : پاکسازی[۲۷] ورودی‌های کاربر در برنامه و بانک اطلاعاتی.

شرح اجمالی

این تنظیم در واقع به معنی یک اعتبار سنجی در فرایندهای ورود داده در database client و سطح برنامه‌ها، از نظر نوع داده، اندازه، قالب و محدوده داده‌ها است. این امکان تا حد زیادی امکان حملات تزریق SQL را کاهش می‌دهد.

نحوه پیاده سازی

با تیم‌های توسعه نرم افزار بررسی شود که در صورت امکان بجای استفاده از فرایندهای ساخت پرس و جوها، از رویه‌های ذخیره شده استفاده شود. همچنین دسترسی‌های غیر ضروری حذف، ثبت و یا تغییر از کاربران گرفته شود. و در صورت امکان پرس و جوهایی بصورت ترکیب رشته‌ها در برنامه ایجاد نشود.

اقدامات زیر می‌تواند آسیب پذیری تزریق SQL را کاهش دهد.

۱- T-SQL و کدهای برنامه را جهت این آسیب پذیری بررسی کنید.

۲- تنها دسترسی‌های محدودی برای شناسه‌هایی که اطلاعات کاربر را به سمت سرور می‌فرستد انتخاب کنید.

۳- در صورت امکان از دستورات مقداری و رویه‌های ذخیره شده استفاده کنید.

[۲۷] Sanitize

۴- رشته‌های ورودی شامل داده‌های باینری، یا کاراکترهای توضیح و صرفنظر[۲۸] را بازگردانید.

۵- هیچگاه از رشته‌های ورودی کاربران، پرس و جو نسازید.

این تغییرات موجب تغییراتی در سمت برنامه و کدهای آن می‌گردد و همواره این تغییرات را بر روی محیط‌های آزمایشگاهی اعمال نمایید و پس از تایید صحت عملکرد به محیط عملیاتی منتقل کنید.

## SCDB-۶-۲ : SAFE_ACCESS برای مشخصه CLR Assembly Permission Set

مشخصه CLR Assembly Permission Set را معادل SAFE_ACCESS برای تمام اسمبلی[۲۹]ها تنظیم نمایید.

### شرح اجمالی

این تنظیم باعث می‌شود، کدهای اسمبلی از دسترسی منابع خارجی مانند فایل‌ها، شبکه متغیرهای محیطی و رجیستری خارج و محفوظ گردد. دسترسی‌های UNSAFE و EXTERNAL_ACCESS امکان آسیب‌های زیادی بر روی سیستم عامل میزبان را ایجاد می‌نماید.

### نحوه پیاده سازی

فرمان زیر را اجرا نمایید:

```
SELECT name, permission_set_desc FROM sys.assemblies where
is_user_defined = 1;
```

خروجی‌های اعلام شده باید دارای مقدار SAFE_ACCESS برای متغیر permission_set_desc باشند.

در صورت فعال نبوده Safe Access برای اسمبلی‌ها، فرمان زیر را برای هر اسمبلی مورد نظر اجرا نمایید:

```
ALTER ASSEMBLY [assembly_name] WITH PERMISSION_SET = SAFE;
```

[۲۸] Comment character and escape sequence
[۲۹] Assembly

## SCDB-۷ : رمزنگاری

SCDB-۷-۱ : انتخاب مقداری برابر یا قوی‌تر از AES128 در پایگاه داده‌های غیر سیستمی برای مشخصه Symmetric Key Encryption Algorithm.

شرح اجمالی

براساس توصیه مایکروسافت در SQL Server به منظور رمزنگاری متقارن تنها باید از رمزنگاری AES موجود با کلیدهایی برابر و یا بالاتر از ۱۲۸ بیت استفاده نمود. این گزینه‌ها عبارتند از AES128، AES192 و AES256.

خیلی از سازمان‌ها ممکن است الگوریتم Triple DES را نیز یک الگوریتم مناسب برای رمزنگاری‌های متقارن بدانند، اما در کل به کارگیری این الگوریتم تقریبا منسوخ شده است. با این حال این الگوریتم همچنان در SQL Server پشتیبانی می‌شود، اما استفاده از AES گزینه پیشنهاد شده می‌باشد.

نحوه پیاده سازی

برای هر پایگاه داده فرمان زیر را اجرا نمایید:

```
USE [dbname]
GO
SELECT db_name() AS Database_Name, name AS Key_Name
FROM sys.symmetric_keys
WHERE algorithm_desc NOT IN ('AES_128','AES_192','AES_256')
AND db_id() > 4 ;
GO
```

در صورت انطباق با این توصیه امنیتی، پس از اجرای فرمان بالا هیچ نتیجه‌ای نباید برگردد.

SCDB-۷-۲ : طول کلید برای الگوریتم‌های نامتقارن در پایگاه داده‌های غیر سیستمی برابر یا بالاتر از ۲۰۴۸ باشد.

شرح اجمالی

براساس توصیه مایکروسافت در SQL Server به منظور استفاده از رمزنگاری نامتقارن باید طول کلید حداقل ۲۰۴۸ بیت باشد.

RSA2048 قویترین الگوریتم برای رمزنگاری نامتقارن در SQL Server می‌باشد و استفاده از این الگوریتم پیشنهاد شده است. سایر الگوریتم‌ها عبارتند از RSA512 و RSA1024 که دارای طول کلید کمتری هستند.

نحوه پیاده سازی

برای هر پایگاه داده فرمان زیر را اجرا نمایید:

```
USE [dbname]
GO
SELECT db_name() AS Database_Name, name AS Key_Name FROM
sys.asymmetric keys
WHERE key_length < 2048
AND db_id() > 4 ;
GO
```

در صورت انطباق با این توصیه امنیتی، پس از اجرای فرمان بالا هیچ نتیجه‌ای نباید برگردد.

## جدول ممیزی

جدول ممیزی خلاصه‌ای از تمامی الزامات بیان شده در متن سند می‌باشد. قابل ذکر است که ستون‌های "وضعیت" و "قابلیت پیاده‌سازی" باید توسط ممیز و برای هر سیستم حاوی این برنامه تکمیل گردد. در ستون وضعیت، ممیز باید از عبارت‌های "قبول" و "رد" متناسب با وضعیت الزام در محصول مورد ارزیابی استفاده نماید. در ستون قابلیت پیاده‌سازی، ممیز باید قابلیت پیاده‌سازی الزام برای محصول مورد ارزیابی را با عبارات "دارد" و "ندارد" بیان نماید. در صورتی که الزامی برای محصول مذکور قابلیت پیاده‌سازی نداشته باشد، علت عدم قابلیت پیاده‌سازی آن باید در ذیل جدول توضیح داده شود.

| شناسه | وضعیت | تنظیمات | قابلیت پیاده سازی | مقدار پیش فرض | مقدار مطلوب |
|---|---|---|---|---|---|
| SCDB-۱ | | نصب و بروز رسانی | | | |
| SCDB-۱-۱ | | بروز رسانی | | ندارد | نصب آخرین بروز رسانی‌ها |
| SCDB-۱-۲ | | نصب بر روی یک سرویس دهنده انحصاری و تک کاربرد صورت گیرد | | ندارد | سرور اختصاصی برای SQL Server |
| SCDB-۲ | | کاهش سطح آسیب پذیری | | | |
| SCDB-۲-۱ | | گزینه Ad Hoc Distributed Queries را غیر فعال کنید | | غیر فعال | غیر فعال |
| SCDB-۲-۲ | | گزینه CLR Enabled را غیر فعال کنید | | غیر فعال | غیر فعال |
| SCDB-۲-۳ | | Cross DB Ownership Chaining را غیرفعال سازید | | غیر فعال | غیر فعال |

| شناسه | وضعیت | تنظیمات | قابلیت پیاده سازی | مقدار پیش فرض | مقدار مطلوب |
|---|---|---|---|---|---|
| SCDB-۲-۴ | | Database Mail XPs را غیرفعال سازید | | غیر فعال | غیر فعال |
| SCDB-۲-۵ | | Ole Automation Procedures را غیرفعال سازید | | غیر فعال | غیر فعال |
| SCDB-۲-۶ | | Remote Access را غیرفعال سازید | | فعال | غیر فعال |
| SCDB-۲-۷ | | Remote Admin Connection را غیرفعال سازید | | غیر فعال | غیر فعال |
| SCDB-۲-۸ | | Scan for Startup Process را غیرفعال سازید | | غیر فعال | غیر فعال |
| SCDB-۲-۹ | | مشخصه Trustworthy بانک اطلاعاتی را غیرفعال سازید | | غیر فعال | غیر فعال |
| SCDB-۲-۱۰ | | پروتکلهای غیر ضروری SQL Server را غیرفعال سازید | | TCP/IP & Shared Memory | TCP/IP |
| SCDB-۲-۱۱ | | SQL Server را با درگاه‌های متفاوت از درگاه‌های پیش فرض تنظیم کنید | | 1433 | غیر از ۱۴۳۳ |
| SCDB-۲-۱۲ | | مشخصه Hide instance بانک اطلاعاتی را فعال نمایید | | غیر فعال | فعال |
| SCDB-۲-۱۳ | | شناسه کاربری sa را غیرفعال نمایید | | فعال | غیر فعال |
| SCDB-۲-۱۴ | | شناسه کاربری sa را تغییر نام دهید | | sa | غیر از sa |
| SCDB-۲-۱۵ | | در تنظیمات سرور امکان xp_cmdshell را غیرفعال نمایید | | غیر فعال | غیر فعال |
| **SCDB-۳** | | **احراز هویت و سنجش سطح دسترسی** | | | |
| SCDB-۳-۱ | | روش احراز هویت سرور را به احراز هویت ویندوز تغییر دهید | | Windows Authentication | Windows Authentication |
| SCDB-۳-۲ | | محدود کردن دسترسی اتصال برای کاربران مهمان | | بدون مجوز اتصال | بدون مجوز اتصال |
| SCDB-۳-۳ | | کاربران اضافی و بدون ارتباط با بانک‌های اطلاعاتی را از روی سرور حذف نمایید | | ندارد | بدون کاربر اضافی |
| SCDB-۳-۴ | | عدم استفاده از SQL authentication برای Contained Database | | Windows Authentication | Windows Authentication |
| SCDB-۳-۵ | | سرویس MSSQL نباید با شناسه کاربری مدیر سیستم یا در سطح مدیر سیستم اجرا شود | | در رده مدیر سیستم نمی‌باشد | در رده مدیر سیستم نباشد |

| شناسه | وضعیت | تنظیمات | قابلیت پیاده سازی | مقدار پیش فرض | مقدار مطلوب |
|---|---|---|---|---|---|
| SCDB-۳-۶ | | سرویس SQLAgent نباید با شناسه کاربری مدیر سیستم یا در سطح مدیر سیستم اجرا شود | | در رده مدیر سیستم نمی‌باشد | در رده مدیر سیستم نباشد |
| SCDB-۳-۷ | | سرویس Full-Text نباید با شناسه کاربری مدیر سیستم یا در سطح مدیر سیستم اجرا شود | | در رده مدیر سیستم نمی‌باشد | در رده مدیر سیستم نباشد |
| **SCDB-۴** | | **قواعد گذرواژه** | | | |
| SCDB-۴-۱ | | مقدار شناسه MUST_CHANGE را برای تمام کاربرهای تایید شده فعال می‌کنیم | | فعال | فعال |
| SCDB-۴-۲ | | فعال سازی CHECK_EXPAIRATION برای تمام کاربرهای دارای نقش Sysadmin | | متغیر | فعال |
| SCDB-۴-۳ | | مقدار شناسه CHECK_POLICY را برای تمام کاربرهای تایید شده فعال نمایید | | فعال | فعال |
| **SCDB-۵** | | **حسابرسی و رویدادنگاری** | | | |
| SCDB-۵-۱ | | مقداردهی مناسب برای بازنویسی فایل‌های رویداد خطا | | ۶ | ۱۲ |
| SCDB-۵-۲ | | تنظیم Default Trace Enable را بر روی سرور بانک اطلاعاتی فعال کنید | | فعال | فعال |
| SCDB-۵-۳ | | امکان رویداد نگاری را برای ورودهای موفق و ناموفق تنظیم نمایید | | فقط ورودهای موفق | ورودهای موفق و ناموفق |
| **SCDB-۶** | | **توسعه نرم افزار** | | | |
| SCDB-۶-۱ | | پاکسازی ورودی‌های کاربر در برنامه و بانک اطلاعاتی | | ندارد | وجود موارد لازم برای پاکسازی ورودی‌ها |
| SCDB-۶-۲ | | SAFE_ACCESS برای مشخصه CLR Assembly Permission Set | | فعال | فعال |
| **SCDB-۷** | | **رمزنگاری** | | | |
| SCDB-۷-۱ | | انتخاب مقداری برابر یا قوی‌تر از AES128 در پایگاه داده‌های غیر سیستمی برای مشخصه Symmetric Key Encryption Algorithm | | ندارد | AES128 |
| SCDB-۷-۲ | | طول کلید برای الگوریتم‌های نامتقارن در پایگاه داده‌های غیر سیستمی برابر یا بالاتر از ۲۰۴۸ باشد | | ندارد | RSA2048 |