Center for Internet Security®

CIS Microsoft SQL Server 2008 R2

v1.4.0 - 09-30-2016

Table of Contents

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft SQL Server 2008 R2 versions – running on Microsoft Windows Server 2008 R2. This guide was tested against Microsoft SQL Server 2008 R2 Service Pack 1 64-bit version. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft SQL Server 2008 R2 on a Microsoft Windows platform.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://community.cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Database Engine**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Editor
Nancy Hidy Wilson
Brian Kelley MCSE, CISA, Security+, Microsoft MVP - SQL Server

Recommendations

1 Updates and Patches

This section contains patching related recommendations.

1.1 Ensure Latest SQL Server Service Packs and Hotfixes are Installed (Not Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

SQL Server patches contain program updates that fix security and product functionality issues found in the software. These patches can be installed with a hotfix which is a single patch, a cumulative update which is a small group of patches or a service pack which is a large collection of patches.
The SQL Server version and patch levels should be the most recent compatible with the organizations' operational needs

Rationale:

Using the most recent SQL Server software, along with all applicable patches can help limit the possibilities for vulnerabilities in the software, the installation version and/or patches applied during setup should be established according to the needs of the organization.

Audit:

To determine your SQL Server service pack level, run the following code snippet.

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

First column returns the installed Service Pack level, the second is the exact build number.

Remediation:

Identify the current version and patch level of your SQL Server instances and ensure they contain the latest security fixes. Make sure to test these fixes in your test environments before updating production instances.

The most recent SQL Server patches can be found here:

Hotfixes and Cumulative updates: http://blogs.msdn.com/b/sqlreleaseservices/

Service Packs: http://support.microsoft.com/kb/968382

Default Value:

Service packs and patches are not installed by default.

References:

1. http://support.microsoft.com/sp
2. http://support.microsoft.com/kb/968382

1.2 Ensure Single-Function Member Servers are Used (Not Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

It is recommended that SQL Server software be installed on a dedicated server. This architectural consideration affords security flexibility in that the database server can be placed on a separate subnet allowing access only from particular hosts and over particular protocols. Degrees of availability are easier to achieve as well - over time, an enterprise can move from a single database server to a failover to a cluster using load balancing or to some combination thereof.

Rationale:

It is easier to manage (i.e. reduce) the attack surface of the server hosting SQL Server software if the only surfaces to consider are the underlying operating system, SQL Server itself, and any security/operational tooling that may additionally be installed. As noted in the description, availability can be more easily addressed if the database is on a dedicated server.

Audit:

Ensure that no other roles are enabled for the underlying operating system and that no excess tooling is installed, per enterprise policy.

Remediation:

Uninstall excess tooling and/or remove unnecessary roles from the underlying operating system.

Impact:

It is difficult to see any reasonably adverse impact to making this architectural change, once the costs of making the change have been paid. Custom applications may need to be modified to accommodate database connections over the wire rather than on the host (i.e. using TCP/IP instead of Named Pipes). Additional hardware and operating system licenses may be required to make these architectural changes.

2 Surface Area Reduction

SQL Server offers various configuration options, some of them can be controlled by the sp_configure stored procedures. This section contains the listing of the corresponding recommendations.

2.1 Ensure 'Ad Hoc Distributed Queries' Server Configuration Option is set to '0' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

Ad Hoc Distributed Queries Allow users to query data and execute statements on external data sources. This functionality should be disabled.

Rationale:

This feature can be used to remotely access and exploit vulnerabilities on remote SQL Server instances and to run unsafe Visual Basic for Application functions.

Audit:

Run the following T-SQL command:

```
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';
```

Both value columns must show 0.

Remediation:

Run the following T-SQL command:

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

Default Value:

0 (disabled)

References:

1. http://msdn.microsoft.com/en-us/library/ms187569(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms187569(v=sql.100).aspx

2.2 Ensure 'CLR Enabled' Server Configuration Option is set to '0' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

The CLR enabled option specifies whether user assemblies can be run by SQL Server.

Rationale:

Enabling use of CLR assemblies widens the attack surface of SQL Server and puts it at risk from both inadvertent and malicious assemblies.

Audit:

Run the following T-SQL command:

```
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';
```

Both value columns must show 0.

Remediation:

Run the following T-SQL command:

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

Default Value:

By default, this option is disabled.

2.3 Ensure 'Cross DB Ownership Chaining' Server Configuration Option is set to '0' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

This option allows controlling cross-database ownership chaining across all databases at the instance (or server) level.

Rationale:

When enabled, this option allows a member of the db_owner role in a database to gain access to objects owned by a login in any other database, causing an unnecessary information disclosure. When required, cross-database ownership chaining should only be enabled for the specific databases requiring it instead of at the instance level for all databases by using the ALTER DATABASE <dbname> SET DB_CHAINING ON command. This database option may not be changed on the master, model, or tempdb system databases.

Audit:

Run the following T-SQL command:

```
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';
```

Both value columns must show 0.

Remediation:

Run the following T-SQL command:

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

Default Value:

0 (disabled)

References:

1. http://msdn.microsoft.com/en-us/library/ms188694(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms188694(v=sql.100).aspx

2.4 Ensure 'Database Mail XPs' Server Configuration Option is set to '0' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

This option controls the generation and transmission of email messages from SQL Server.

Rationale:

Disabling Database Mail reduces the SQL Server surface, eliminates a DOS attack vector and channel to exfiltrate data from the database server to a remote host.

Audit:

Run the following T-SQL command:

```
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';
```

Both value columns must show 0.

Remediation:

Run the following T-SQL command:

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

Default Value:

By default, this option is disabled.

References:

1. http://msdn.microsoft.com/en-us/library/ms175887(v=sql.105)

2.5 Ensure 'Ole Automation Procedures' Server Configuration Option is set to '0' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

Extended stored procedures that allow SQL Server users to execute functions external to SQL Server.

Rationale:

Enabling this option will increase the attack surface of SQL Server and allow users to execute functions in the security context of SQL Server.

Audit:

```
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';
```

Both value columns must show 0.

Remediation:

Run the following T-SQL command:

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

Default Value:

0 (disabled)

References:

1. http://msdn.microsoft.com/en-us/library/ms191188(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms191188(v=sql.100).aspx

2.6 Ensure 'Remote Access' Server Configuration Option is set to '0' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

Enables the execution of local stored procedures on remote servers or remote stored procedures on local server.

Rationale:

Functionality can be abused to launch a Denial-of-Service (DoS) attack on remote servers by off-loading query processing to a target.

Audit:

Run the following T-SQL command:

```
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';
```

Both value columns must show 0.

Remediation:

Run the following T-SQL command:

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

Default Value:

1 (enabled)

References:

1. http://msdn.microsoft.com/en-us/library/ms187660(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms187660(v=sql.100).aspx

2.7 Ensure 'Remote Admin Connections' Server Configuration Option is set to '0' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

This setting controls whether a client application on a remote computer can use the Dedicated Administrator Connection (DAC).

Rationale:

The Dedicated Administrator Connection (DAC) lets an administrator access a running server to execute diagnostic functions or Transact-SQL statements, or to troubleshoot problems on the server, even when the server is locked or running in an abnormal state and not responding to a SQL Server Database Engine connection. In a cluster scenario the administrator may not actually be logged on to the same node that is currently hosting the SQL Server instance and thus is considered "remote". Therefore, this setting should usually be enabled (1) for SQL Server failover clusters; otherwise it should be disabled (0) which is the default.

Audit:

Run the following T-SQL command:

```
USE master;
GO
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;
```

If no data is returned, the instance is a cluster and this recommendation is not applicable. If data is returned, then both the value columns must show 0.

Remediation:

Run the following command on non-clustered installations:

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

Default Value:

0 (disabled)

References:

1. http://msdn.microsoft.com/en-us/library/ms190468(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms190468(v=sql.100).aspx

2.8 Ensure 'Scan for Startup Procs' Server Configuration Option is set to '0' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

This option causes SQL Server to scan for and automatically run all stored procedures that are set to execute upon service startup.

Rationale:

Enforcing this control reduces the threat of an entity leveraging these facilities for malicious purposes.

Audit:

Run the following T-SQL command:

```
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';
```

Both value columns must show 0.

Remediation:

Run the following T-SQL command:

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

Impact:

Setting Scan for Startup Procedures to 0 will prevent certain audit traces and other commonly used monitoring SPs from re-starting on start up. Additionally, replication requires this setting to be enabled (1) and will automatically change this setting if needed.

Default Value:

0 (disabled)

References:

1. http://msdn.microsoft.com/en-us/library/ms179460(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms179460(v=sql.100).aspx

2.9 Ensure 'SQL Mail XPs' Server Configuration Option is set to '0' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

SQL Mail provides a mechanism to send, receive, delete, and process e-mail messages using SQL Server.

Rationale:

SQL Mail, which is deprecated in favor of Database Mail and if disabled reduces the SQL Server surface, eliminates a DOS attack vector and channel to exfiltrate data from the database server to a remote host.

Audit:

Run the following T-SQL command:

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

Both value columns must show 0.

Remediation:

Run the following T-SQL command:

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

Default Value:

0 (disabled)

References:

1. http://msdn.microsoft.com/en-us/library/ms190755(v=sql.105).aspx

2. http://msdn.microsoft.com/en-us/library/ms190755(v=sql.100).aspx

2.10 Ensure 'Trustworthy' Database Property is set to 'Off' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

The TRUSTWORTHY option allows database objects to access objects in other database under certain circumstances.

Rationale:

Provides protection from malicious CLR assemblies or extended procedures.

Audit:

Run the following T-SQL query to list any databases with a Trustworthy database property value of ON:

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

No rows should be returned.

Remediation:

Execute the following statement against the databases returned by the Audit Procedure:

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

Default Value:

OFF

References:

1. http://msdn.microsoft.com/en-us/library/ms187861(v=sql.100).aspx
2. http://msdn.microsoft.com/en-us/library/ms187861(v=sql.105).aspx

2.11 Ensure Unnecessary SQL Server Protocols are set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

SQL Server supports Shared Memory, Named Pipes, TCP/IP and VIA protocols. However, SQL Server should be configured to use the bare minimum required based on the organization's needs.

Rationale:

Using fewer protocols minimizes the attack surface of SQL Server and in some cases can protect it from remote attacks.

Audit:

Open SQL Server Configuration Manager; go to the SQL Server Network Configuration. Ensure that only required protocols are enabled.

Remediation:

Open SQL Server Configuration Manager; go to the SQL Server Network Configuration. Ensure that only required protocols are enabled. Disable protocols not necessary.

Impact:

The Database Engine must be stopped and restarted for the change to take effect.

Default Value:

By default, TCP/IP and Shared Memory protocols are enabled on all commerical SQL Server 2008 instances.

References:

1. http://msdn.microsoft.com/en-us/library/ms191294(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms191294(v=sql.100).aspx

2.12 Ensure SQL Server is configured to use non-standard ports (Not Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

If enabled, the default SQL Server instance will be assigned a default port of TCP:1433 for TCP/IP communication. Administrators can also configure named instances to use TCP:1433 for communication. TCP:1433 is a widely known SQL Server port and this port assignment should be changed.

Rationale:

Using a non-default port helps protect the database from attacks directed to the default port.

Audit:

Open a PowerShell window and run the following command:

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

This should return no lines. If any lines returned, check the process id in the last column if it's a SQL Server instance.

Remediation:

1. In SQL Server Configuration Manager, in the console pane, expand SQL Server Network Configuration, expand Protocols for, and then double-click the TCP/IP or VIA protocol
2. In the TCP/IP Properties dialog box, on the IP Addresses tab, several IP addresses appear in the format IP1, IP2, up to IPAll. One of these is for the IP address of the loopback adapter, 127.0.0.1. Additional IP addresses appear for each IP Address on the computer
3. Change the TCP Port field from 1433 to another non-standard port or leave the TCP Port field empty and set the TCP Dynamic Ports value to 0 to enable dynamic port assignment and then click OK.
4. In the console pane, click SQL Server Services.
5. In the details pane, right-click SQL Server () and then click Restart, to stop and restart SQL Server.

Impact:

Changing the default port will force DAC (Default Administrator Connection) to listen on a random port. Also, it might make benign applications, such as application firewalls, require special configuration.

Default Value:

By default, default SQL Server instances listen on to TCP/IP traffic on TCP port 1433 and named instances use dynamic ports.

References:

1. http://support.microsoft.com/kb/308091
2. http://msdn.microsoft.com/en-us/library/ms177440(v=sql.105).aspx
3. http://msdn.microsoft.com/en-us/library/ms177440(v=sql.100).aspx

2.13 Ensure 'Hide Instance' option is set to 'Yes' for Production SQL Server instances (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

Non-clustered SQL Server instances within production environments should be designated as hidden to prevent advertisement by the SQL Server Browser service.

Rationale:

Designating production SQL Server instances as hidden leads to a more secure installation because they cannot be enumerated. However, clustered instances may break if this option is selected.

Audit:

1. In SQL Server Configuration Manager, expand SQL Server Network Configuration, right-click Protocols for <server instance>, and then select Properties.
2. On the Flags tab, in the Hide Instance box, verify Yes is selected.

OR

Execute the following T-SQL. A value of 1 should be returned.

```
DECLARE @getValue INT;
EXEC master..xp_instance_regread
      @rootkey = N'HKEY_LOCAL_MACHINE',
      @key = N'SOFTWARE\Microsoft\Microsoft SQL Server\MSSQLServer\SuperSocketNetLib',
      @value_name = N'HideInstance',
      @value = @getValue OUTPUT;
SELECT @getValue;
```

Remediation:

1. In SQL Server Configuration Manager, expand SQL Server Network Configuration, right-click Protocols for <server instance>, and then select Properties.
2. On the Flags tab, in the Hide Instance box, select Yes, and then click OK to close the dialog box. The change takes effect immediately for new connections.

OR

Execute the following T-SQL to remediate:

```
EXEC master..xp_instance_regwrite
      @rootkey = N'HKEY_LOCAL_MACHINE',
      @key = N'SOFTWARE\Microsoft\Microsoft SQL Server\MSSQLServer\SuperSocketNetLib',
      @value_name = N'HideInstance',
      @type = N'REG_DWORD',
      @value = 1;
```

Impact:

This method only prevents the instance from being listed on the network. If the instance is hidden (not exposed by SQL Browser), then connections will need to specify the server and port in order to connect. It does not prevent users from connecting to server if they know the instance name and port.

If you hide a clustered named instance, the cluster service may not be able to connect to the SQL Server. Please refer to the Microsoft documentation reference.

Default Value:

By default, SQL Server instances are not hidden.

References:

1. http://msdn.microsoft.com/en-us/library/ms179327(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms179327(v=sql.100).aspx

2.14 Ensure 'sa' Login Account is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

The `sa` account is a widely known and often widely used SQL Server account with sysadmin privileges.

Rationale:

Enforcing this control reduces the probability of an attacker executing brute force attacks against a well-known principal.

Audit:

Use the following syntax to determine if the sa account is disabled.

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

An is_disabled value of 1 indicates the account is currently disabled.

Remediation:

Execute the following query:

```
ALTER LOGIN sa DISABLE;
```

Impact:

It is not a good security practice to code applications or scripts to use the sa account. However, if this has been done disabling the sa account will prevent scripts and applications for authenticating to the database server and executing required tasks or functions.

Default Value:

By default, the '`sa' login` account is enabled.

References:

1. http://msdn.microsoft.com/en-us/library/ms188786(v=sql.100).aspx

2. http://msdn.microsoft.com/en-us/library/ms188786(v=sql.105).aspx
3. http://msdn.microsoft.com/en-us/library/ms189828(v=sql.100).aspx
4. http://msdn.microsoft.com/en-us/library/ms189828(v=sql.105).aspx

2.15 Ensure 'sa' Login Account has been renamed (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

The `sa` account is a widely known and often widely used SQL Server account with sysadmin privileges.

Rationale:

It is more difficult to launch password-guessing and brute-force attacks against the sa account if the username is not known.

Audit:

Use the following syntax to determine if the sa account is renamed.

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

A name of sa indicates the account has not been renamed.

Remediation:

Replace the different_user value within the below syntax and execute rename the sa login.

```
ALTER LOGIN sa WITH NAME = different_user;
```

Impact:

It is not a good security practice to code applications or scripts to use the sa account. However, if this has been done renaming the sa account will prevent scripts and applications for authenticating to the database server and executing required tasks or functions.

Default Value:

By default, the '`sa`' account name is 'sa'

References:

1. http://msdn.microsoft.com/en-us/library/ms144284.aspx

2.16 Ensure 'xp_cmdshell' Server Configuration Option is set to '0' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

The xp_cmdshell procedure allows an authenticated SQL Server user to execute operating-system command shell commands and return results as rows within the SQL client.

Rationale:

xp_cmdshell is commonly used by attackers to read or write data to/from the underlying Operating System of a database server.

Audit:

Run the following code snippet to determine if the xp_cmdshell system stored procedure is enabled:

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

A run value of 0 indicates that the xp_cmdshell option is disabled. If the option is enabled, run the following code snippet to disable this option:

```
EXECUTE sp_configure 'show advanced options',1;
RECONFIGURE WITH OVERRIDE;
EXECUTE sp_configure 'xp_cmdshell',0;
RECONFIGURE WITH OVERRIDE;
```

Remediation:

Run the following T-SQL command:

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

Default Value:

0 (disabled)

References:

1. http://msdn.microsoft.com/en-us/library/ms175046(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms175046(v=sql.100).aspx
3. http://msdn.microsoft.com/en-us/library/ms190693(v=sql.105).aspx
4. http://msdn.microsoft.com/en-us/library/ms190693(v=sql.100).aspx

3 Authentication and Authorization

This section contains authentication and authorization related recommendations.

3.1 Ensure 'Server Authentication' Property is set to 'Windows Authentication mode' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

Uses Windows Authentication to validate attempted connections.

Rationale:

Windows provides a more robust authentication mechanism than SQL Server authentication.

Audit:

Execute the following syntax:

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

A config_value of Windows NT Authentication indicates the Server Authentication property is set to Windows Authentication mode

Remediation:

Perform the following steps:

1. Open SQL Server Management Studio.
2. Open the Object Explorer tab and connect to the target database instance.
3. Right click the instance name and select Properties.
4. Select the Security page from the left menu.
5. Set the Server authentication setting to Windows Authentication mode.

Default Value:

Windows Authentication Mode

References:

1. http://msdn.microsoft.com/en-us/library/ms188470(v=sql.100).aspx

2. http://msdn.microsoft.com/en-us/library/ms188470(v=sql.105).aspx

3.2 Ensure CONNECT permissions on the 'guest user' is Revoked within all SQL Server databases excluding the master, msdb and tempdb (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

Removes the right of guest users to connect to SQL Server user databases.

Rationale:

A login assumes the identity of the guest user when a login has access to SQL Server but does not have access to a database through its own account and the database has a guest user account. Revoking the connect permission for the guest user will ensure that a login is not able to access database information without explicit access to do so.

Audit:

Run the following code snippet in each database in the instance to determine if the guest user has CONNECT permission. No rows should be returned.

```
USE [database_name];
GO
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';
```

Remediation:

The following code snippet revokes CONNECT permissions from the guest user in a database:

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

Impact:

When CONNECT permission to the guest user is revoked, a SQL Server instance login must be mapped to a database user explicitly in order to have access to the database.

Default Value:

The guest user account is added to each new database but without CONNECT permission by default.

References:

1. http://msdn.microsoft.com/en-us/library/bb402861(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/bb402861(v=sql.100).aspx

3.3 Ensure 'Orphaned Users' are Dropped From SQL Server Databases (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

A database user for which the corresponding SQL Server login is undefined or is incorrectly defined on a server instance cannot log in to the instance and is referred to as orphaned and should be removed.

Rationale:

Orphan users should be removed to avoid potential misuse of those broken users in any way.

Audit:

Run the following T-SQL query to identify orphan users. No rows should be returned.

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

Remediation:

Run the following T-SQL query to remove an orphan user:

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

References:

1. http://msdn.microsoft.com/en-us/library/ms175475(v=sql.100).aspx
2. http://msdn.microsoft.com/en-us/library/ms175475(v=sql.105).aspx

4 Password Policies

This section contains recommendations related to password policies.

4.1 Ensure 'MUST_CHANGE' Option is set to 'ON' for All SQL Authenticated Logins (Not Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

SQL Server will prompt for an updated password the first time the altered login is used.

Rationale:

Enforcing password change will prevent the account administrators or anyone accessing the initial password to misuse the SQL login created without being noticed.

Audit:

1. Open SQL Server Management Studio.
2. Open Object Explorer and connect to the target instance.
3. Navigate to the Logins tab in Object Explorer and expand. Right click on the desired login and select Properties.
4. Verify the User must change password at next login checkbox is checked

Remediation:

Set the MUST_CHANGE option for SQL Authenticated logins

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

Impact:

CHECK_EXPIRATION and CHECK_POLICY options must both be ON

Default Value:

ON

References:

1. http://msdn.microsoft.com/en-us/library/ms189828(v=sql.105).aspx

2. http://msdn.microsoft.com/en-us/library/ms189828(v=sql.100).aspx

4.2 Ensure 'CHECK_EXPIRATION' Option is set to 'ON' for All SQL Authenticated Logins Within the Sysadmin Role (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

Applies the same password expiration policy used in Windows to passwords used inside SQL Server.

Rationale:

Ensuring SQL logins comply with the secure password policy applied by the Windows Server Benchmark will ensure the passwords for SQL logins with Sysadmin privileges are changed on a frequent basis to help prevent compromise via a brute force attack.

Audit:

Run the following T-SQL statement to find sysadmin logins with CHECK_EXPIRATION OFF. No rows should be returned.

```
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;
```

Remediation:

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

Impact:

This is a mitigating recommendation for systems which cannot follow the recommendation to use only Windows Authenticated logins.

In regards to limiting this rule to only logins with sysadmin and CONTROL SERVER privileges, there are too many cases of applications that run with less than sysadmin level privileges that have hard-coded passwords or effectively hard-coded passwords (whatever

is set the first time is nearly impossible to change). There are several line of business applications that are considered best of breed which has this failing.

Also, keep in mind that the password policy is taken from the computer's local policy, which will take from the Default Domain Policy setting. Many organizations have a different password policy with regards to service accounts. These are handled in AD by setting the account's password not to expire and having some other process track when they need to be changed. With this second control in place, this is perfectly acceptable from an audit perspective. If you treat a SQL Server login as a service account, then you have to do the same. This ensures that the password change happens during a communicated downtime window and not arbitrarily.

Default Value:

'CHECK_EXPIRATION' is ON

References:

1. http://msdn.microsoft.com/en-us/library/ms161959(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms161959(v=sql.100).aspx

4.3 Ensure 'CHECK_POLICY' Option is set to 'ON' for All SQL Authenticated Logins (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

Applies the same password complexity policy used in Windows to passwords used inside SQL Server.

Rationale:

Ensuring SQL logins comply with the secure password policy applied by the Windows Server Benchmark will ensure SQL logins are not blank and cannot be easily compromised via brute force attack.

Audit:

Use the following code snippet to determine the SQL Logins and if their password complexity is enforced.

```
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';
```

A PasswordPolicyEnforced value of 0 indicates that the 'Check_Policy' option is OFF

Remediation:

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

Default Value:

'CHECK_POLICY' is ON

References:

1. http://msdn.microsoft.com/en-us/library/ms161959(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms161959(v=sql.100).aspx

5 Auditing and Logging

SQL Server audit and logging configuration settings.

5.1 Ensure 'Maximum number of error log files' is set to greater than or equal to '12' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

SQL Server errorlog files must be protected from loss. The log files must be backed up before they are overwritten. Retaining more errorlogs helps prevent loss from frequent recycling before backups can occur.

Rationale:

The SQL Server errorlog contains important information about major server events and login attempt information as well.

Audit:

1. Open SQL Server Management Studio.
2. Open Object Explorer and connect to the target instance.
3. Navigate to the Management tab in Object Explorer and expand. Right click on the SQL Server Logs file and select Configure.
4. Verify the Limit the number of error log files before they are recycled checkbox is checked
5. Verify the Maximum number of error log files is greater than or equal to 12

OR

Run the following T-SQL. The NumberOfLogFiles returned should be greater than or equal to 12.

```
DECLARE @NumErrorLogs int;
EXEC master.sys.xp_instance_regread
N'HKEY_LOCAL_MACHINE',
N'Software\Microsoft\MSSQLServer\MSSQLServer',
N'NumErrorLogs',
@NumErrorLogs OUTPUT;

SELECT ISNULL(@NumErrorLogs, -1) AS [NumberOfLogFiles];
```

Remediation:

Adjust the number of logs to prevent data loss. The default value of 6 may be insufficient for a production environment.

1. Open SQL Server Management Studio.
2. Open Object Explorer and connect to the target instance.
3. Navigate to the Management tab in Object Explorer and expand. Right click on the SQL Server Logs file and select Configure
4. Check the Limit the number of error log files before they are recycled
5. Set the Maximum number of error log files to greater than or equal to 12

OR

Run the following T-SQL to change the number of error log files, replace <NumberAbove12> with your desired number of error log files:

```
EXEC master.sys.xp_instance_regwrite
N'HKEY_LOCAL_MACHINE',
N'Software\Microsoft\MSSQLServer\MSSQLServer',
N'NumErrorLogs',
REG_DWORD,
<NumberAbove12>;
```

Impact:

Once the max number of errorlogs is reached, the oldest errorlog file is deleted each time SQL Server restarts or sp_cycle_errorlog is executed.

Default Value:

6 SQL Server errorlog files in addition to the current errorlog file are retained by default.

References:

1. http://msdn.microsoft.com/en-us/library/ms177285(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms177285(v=sql.100).aspx

5.2 Ensure 'Default Trace Enabled' Server Configuration Option is set to '1' (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

The default trace provides audit logging of database activity including account creations, privilege elevation and execution of DBCC commands.

Rationale:

Default trace provides valuable audit information regarding security-related activities on the server.

Audit:

Run the following T-SQL command:

```
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';
```

Both value columns must show 1.

Remediation:

Run the following T-SQL command:

```
EXECUTE sp_configure 'show advanced options', 1;
RECONFIGURE;
EXECUTE sp_configure 'Default trace enabled', 1;
RECONFIGURE;
GO
EXECUTE sp_configure 'show advanced options', 0;
RECONFIGURE;
```

Default Value:

1 (on)

References:

1. http://msdn.microsoft.com/en-us/library/ms175513(v=sql.105).aspx

2. http://msdn.microsoft.com/en-us/library/ms175513(v=sql.100).aspx

5.3 Ensure 'Login Auditing' is set to Both 'failed' and 'successful logins' (Not Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

Setting logs both successful and failed login SQL Server authentication attempts.

Rationale:

Logging successful and failed logins provides key information that can be used to detect\confirm password guessing attacks. Further, logging successful login attempts can be used to confirm server access during forensic investigations.

Audit:

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

A config_value of 'all' indicates a server login auditing setting of 'Both failed and successful logins'.

Remediation:

Perform the following steps to set the level of auditing:

1. Open SQL Server Management Studio.
2. Right click the target instance and select Properties and navigate to the Security tab.
3. Select the option `Both failed and successful logins` under the "Login Auditing" section and click OK.
4. Restart the SQL Server instance.

Default Value:

By default, only failed login attempted are captured.

References:

1. http://technet.microsoft.com/en-us/library/ms188470(v=sql.105).aspx
2. http://technet.microsoft.com/en-us/library/ms188470(v=sql.100).aspx

6 Application Development

This section contains application developed related recommendations.

6.1 Ensure Sanitize Database and Application User Input is Sanitized (Not Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

Always validate user input received from a database client or application by testing type, length, format, and range prior to transmitting it to the database server.

Rationale:

Sanitizing user input drastically minimizes risk of SQL injection.

Audit:

Check with the application teams to ensure any database interaction is through the use of stored procedures and not dynamic SQL. Revoke any INSERT, UPDATE, or DELETE privileges to users so that modifications to data must be done through stored procedures. Verify that there's no SQL query in the application code produced by string concatenation.

Remediation:

The following steps can be taken to remediate SQL injection vulnerabilities:

- Review TSQL and application code for SQL Injection
- Only permit minimally privileged accounts to send user input to the server
- Minimize the risk of SQL injection attack by using parameterized commands and stored procedures
- Reject user input containing binary data, escape sequences, and comment characters
- Always validate user input and do not use it directly to build SQL statements

Impact:

Sanitize user input may require changes to application code or database object syntax. These changes can require applications or databases to be taken temporarily off-line. Any

change to TSQL or application code should be thoroughly tested in testing environment before production implementation.

References:

1. https://www.owasp.org/index.php/SQL_Injection
2. http://msdn.microsoft.com/en-us/library/ms161953(v=sql.100).aspx
3. http://msdn.microsoft.com/en-us/library/ms161953(v=sql.105).aspx

6.2 Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies (Scored)

Profile Applicability:

- Level 1 - Database Engine

Description:

Setting CLR Assembly Permission Sets to SAFE_ACCESS will prevent assemblies from accessing external system resources such as files, the network, environment variables, or the registry.

Rationale:

Assemblies with EXTERNAL_ACCESS or UNSAFE permission sets can be used to access sensitive areas of the operating system, steal and/or transmit data and alter the state and other protection measures of the underlying Windows Operating System.

Assemblies which are Microsoft-created (is_user_defined = 0) are excluded from this check as they are required for overall system functionality.

Audit:

Execute the following SQL statement:

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

All the returned assemblies should show SAFE_ACCESS in the permission_set_desc column.

Remediation:

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

Impact:

The remediation measure should first be tested within a test environment prior to production to ensure the assembly still functions as designed with SAFE permission setting.

Default Value:

SAFE permission set

References:

1. http://msdn.microsoft.com/en-us/library/ms345101(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms189790(v=sql.100).aspx
3. http://msdn.microsoft.com/en-us/library/ms189790(v=sql.105).aspx
4. http://msdn.microsoft.com/en-us/library/ms345101(v=sql.100).aspx
5. http://msdn.microsoft.com/en-us/library/ms186711(v=sql.100).aspx
6. http://msdn.microsoft.com/en-us/library/ms186711(v=sql.105).aspx

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Updates and Patches**		
1.1	Ensure Latest SQL Server Service Packs and Hotfixes are Installed (Not Scored)	☐	☐
1.2	Ensure Single-Function Member Servers are Used (Not Scored)	☐	☐
2	**Surface Area Reduction**		
2.1	Ensure 'Ad Hoc Distributed Queries' Server Configuration Option is set to '0' (Scored)	☐	☐
2.2	Ensure 'CLR Enabled' Server Configuration Option is set to '0' (Scored)	☐	☐
2.3	Ensure 'Cross DB Ownership Chaining' Server Configuration Option is set to '0' (Scored)	☐	☐
2.4	Ensure 'Database Mail XPs' Server Configuration Option is set to '0' (Scored)	☐	☐
2.5	Ensure 'Ole Automation Procedures' Server Configuration Option is set to '0' (Scored)	☐	☐
2.6	Ensure 'Remote Access' Server Configuration Option is set to '0' (Scored)	☐	☐
2.7	Ensure 'Remote Admin Connections' Server Configuration Option is set to '0' (Scored)	☐	☐
2.8	Ensure 'Scan For Startup Procs' Server Configuration Option is set to '0' (Scored)	☐	☐
2.9	Ensure 'SQL Mail XPs' Server Configuration Option is set to '0' (Scored)	☐	☐
2.10	Ensure 'Trustworthy' Database Property is set to 'Off' (Scored)	☐	☐
2.11	Ensure Unnecessary SQL Server Protocols are set to 'Disabled' (Not Scored)	☐	☐
2.12	Ensure SQL Server is configured to use non-standard ports (Not Scored)	☐	☐
2.13	Ensure 'Hide Instance' option is set to 'Yes' for Production SQL Server instances (Scored)	☐	☐
2.14	Ensure 'sa' Login Account is set to 'Disabled' (Scored)	☐	☐
2.15	Ensure 'sa' Login Account has been renamed (Scored)	☐	☐
2.16	Ensure 'xp_cmdshell' Server Configuration Option is set to '0' (Scored)	☐	☐
3	**Authentication and Authorization**		
3.1	Ensure 'Server Authentication' Property is set to 'Windows	☐	☐

	Authentication mode' (Scored)		
3.2	Ensure CONNECT permissions on the 'guest user' is Revoked within all SQL Server databases excluding the master, msdb and tempdb (Scored)	☐	☐
3.3	Ensure 'Orphaned Users' are Dropped From SQL Server Databases (Scored)	☐	☐
4	**Password Policies**		
4.1	Ensure 'MUST_CHANGE' Option is set to 'ON' for All SQL Authenticated Logins (Not Scored)	☐	☐
4.2	Ensure 'CHECK_EXPIRATION' Option is set to 'ON' for All SQL Authenticated Logins Within the Sysadmin Role (Scored)	☐	☐
4.3	Ensure 'CHECK_POLICY' Option is set to 'ON' for All SQL Authenticated Logins (Scored)	☐	☐
5	**Auditing and Logging**		
5.1	Ensure 'Maximum number of error log files' is set to greater than or equal to '12' (Scored)	☐	☐
5.2	Ensure 'Default Trace Enabled' Server Configuration Option is set to '1' (Scored)	☐	☐
5.3	Ensure 'Login Auditing' is set to Both 'failed' and 'successful logins' (Not Scored)	☐	☐
6	**Application Development**		
6.1	Ensure Sanitize Database and Application User Input is Sanitized (Not Scored)	☐	☐
6.2	Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies (Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
11-30-2012	1.1.0	Fixed conflict between recommendation 2.7 name and description
11-30-2012	1.1.0	Removed Level 2 profile from the benchmark.
11-30-2012	1.1.0	Updated audit query, default value and impact for recommendation 4.2 to clarify that only the guest user with CONNECT permission is in scope.
09-06-2014	1.2.0	Removed section "3 Extended Stored Procedures" per Ticket #109
09-06-2014	1.2.0	Updated 2.8 "Scan for Startup Procs" per Ticket #110
09-06-2014	1.2.0	Added recommendation to "Install on dedicated single-function member servers" per Ticket #115
09-06-2014	1.2.0	Updated 2.3 per Ticket #99
09-06-2014	1.2.0	Moved xp_cmdshell recommendation in to Section 2 per Ticket #116
10-09-2015	1.3.0	Add Clarification to Recommendation 6.2 Ticket #139
09-30-2016	1.4.0	Fixed Recommendation 2.13, Audit and Remediation are the same Ticket #146
09-30-2016	1.4.0	Add 5.1 Set the 'Maximum number of error log files' setting to greater than

		or equal to 12 Ticket #143
09-30-2016	1.4.0	Updated 2.12 Set the 'Hide Instance' option to 'Yes' for Production SQL Server instances Ticket #149
09-30-2016	1.4.0	Updated Titles to conform with the CIS Standard.