Security Benchmarks™
A DIVISION OF CENTER FOR INTERNET SECURITY

CIS Microsoft SQL Server 2008 R2 Database

v1.0.0

Export Date 11-13-2012

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document, Security Configuration Benchmark for Microsoft SQL Server 2008, provides prescriptive guidance for establishing a secure configuration posture for Microsoft SQL Server 2008 versions – running on Microsoft Windows Server 2008 R2. This guide was tested against Microsoft SQL Server 2008 64-bit version 10.00.5500 (Service Pack 3) as installed by Microsoft SQL Server 2008 Service Pack 3. 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 on a Microsoft Windows platform.

Consensus Guidance

This benchmark was created using a consensus review process comprised of volunteer and contract 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 released to the public Internet. 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 review process, please send us a note to feedback@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**

  System administrators with any level of security knowledge and experience can understand and perform the specified actions. The action is unlikely to cause an interruption of service to the operating system or the applications that run on it. The actions can be automatically monitored, and the configuration verified, by Scoring Tools that are available from the Center or by CIS-certified Scoring Tools.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

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:

Author
Erik Bitemo
Kevvie Fowler

Contributor
Nancy Wilson
Tung Bui Viet
Chris Bielinski
Sheila Christman
KiÃtzul Flores
Louis Lam
Jin Cao
Chris Bielinski
Brian Kelley
Jorge Gallardo
Tung Bui Viet
Justin Brown
Andrea Weber
Masoud Sultan
Kevin Zhang

Editor
Susan Jordan

Recommendations

1 Updates and Patches

[This space intentionally left blank]

1.1 Install the Latest SQL Server Service Packs and Hotfixes (Not Scored)

Profile Applicability:

- Level 1

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

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 Set the 'Ad Hoc Distributed Queries' Server Configuration Option to 0 (Scored)

Profile Applicability:

- Level 1

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;
```

References:

1. http://msdn.microsoft.com/en-us/library/ms187569(v=sql.105).aspx
2. http://msdn.microsoft.com/en-us/library/ms187569%28v=SQL.100%29.aspx

2.2 Set the 'CLR Enabled' Server Configuration Option to 0 (Scored)

Profile Applicability:

- Level 1

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;
```

2.3 Set the 'Cross DB Ownership Chaining' Server Configuration Option to 0 (Scored)

Profile Applicability:

- Level 1

Description:

This option allows controlling cross-database ownership chaining across all databases.

Rationale:

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.

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
```

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 Set the 'Database Mail XPs' Server Configuration Option to 0 (Scored)

Profile Applicability:

- Level 1

Description:

Enables 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;
```

2.5 Set the 'Ole Automation Procedures' Server Configuration Option to 0 (Scored)

Profile Applicability:

- Level 1

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';
```

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;
```

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 Set the 'Remote Access' Server Configuration Option to 0 (Scored)

Profile Applicability:

- Level 1

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;
```

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 Set the 'Remote Admin Connections' Server Configuration Option to 0 (Scored)

Profile Applicability:

- Level 1

Description:

This option defines whether the Dedicated Admin Connection (DAC) is listening on localhost only or on the SQL Server IP address. If it's a clustered installation, it must be enabled as a clustered SQL Server cannot bind to localhost and DAC will be unavailable otherwise. Enable it for clustered installations. Disable it for standalone installations where not required.

Rationale:

The Dedicated Admin Connection is a powerful database feature that allows connected users to circumvent the SQL Server abstraction layer and have direct access to several system tables which can be used to conduct malicious activities. This feature should be restricted to local administration only to reduce exposure.

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 admin connections';
```

Both value columns must show 1 on clustered installations.

Remediation:

Run the following T-SQL command on clustered installations:

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

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 Set the 'Scan For Startup Procs' Server Configuration Option to 0 (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

This is a defense in depth measure to reduce 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.

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 Set the 'SQL Mail XPs' Server Configuration Option to 0 (Scored)

Profile Applicability:

- Level 1

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;
```

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

2.10 Set the 'Trustworthy' Database Property To Off (Scored)

Profile Applicability:

- Level 1

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 the database with a Trustworthy database property value of ON:

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

Remediation:

Execute the following statement against the database:

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

References:

1. http://msdn.microsoft.com/en-us/library/ms187861%28v=SQL.100%29.aspx

2.11 Disable Unnecessary SQL Server Protocols (Not Scored)

Profile Applicability:

- Level 1

Description:

SQL Server supports Shared Memory, Named Pipes, TCP/IP and VIA protocols however should be configured to use the bare minimum required based on the organizations 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

References:

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

2.12 Configure SQL Server to use non-standard ports (Not Scored)

Profile Applicability:

- Level 1

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 <instance name>, 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 Dyanmic 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 (<instance name>) and then click Restart, to stop and restart SQL Server.

Impact:

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

References:

1. http://msdn.microsoft.com/en-us/library/ms177440%28v=SQL.100%29.aspx
2. http://support.microsoft.com/kb/308091

2.13 Set the 'Hide Instance' option to 'Yes' for Production SQL Server instances (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

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.

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, select Yes, and then click OK to close the dialog box. The change takes effect immediately for new connections.

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.

2.14 Rename the 'sa' Login Account (Scored)

Profile Applicability:

- Level 1

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 to disable and 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.

2.15 Disable the 'sa' Login Account (Scored)

Profile Applicability:

- Level 1

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

A is_disabled value of 0 indicates the account is currently disabled.

Remediation:

```
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 renaming the sa account will prevent scripts and applications for authenticating to the database server and executing required tasks or functions.

References:

1. http://msdn.microsoft.com/en-us/library/aa905197(v=SQL.80).aspx

2.

3 Extended Stored Procedures

Extended stored procedures are to be removed in a future version of SQL Server. They should be avoided at all in new development work or long-term operations. Consider using CLR Integration instead. The following extended stored procedures should not be used by any application or maintenance script. Do not attempt to remove or assign DENY rule to any of these stored procedures. Doing so may result in an unsupported installation of SQL Server 2008.

3.1 Disable the 'xp_availablemedia' procedure (Scored)

Profile Applicability:

- Level 1

Description:

Lists all available storage devices that may be written to

Rationale:

Ensuring this procedure is disabled will prevent an attacker from viewing local available drives for directory and file enumeration. This procedure is currently leveraged by several automated SQL Injection tools

Audit:

To view the permissions for this stored procedure, perform the following steps in SQL Server Management Studio:

1. In Object Explorer, navigate to the SQL Server instance and expand the path: `Databases\System Databases\master\Programmability\Extended` Stored Procedures
2. Locate `xp_availablemedia`, right click and select Properties.
3. The permissions for this extended stored procedure can be viewed in the Permissions tab.

Remediation:

Revoke use by all general users on the SQL Server machine:

```
REVOKE EXECUTE ON xp_availablemedia TO PUBLIC;
```

Note: Server logins within the sysadmin role will retain use of this procedure

3.2 Set the 'xp_cmdshell' option to disabled (Scored)

Profile Applicability:

- Level 1

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;
```

References:

1. http://msdn.microsoft.com/en-us/library/ms175046(v=sql.110).aspx
2. http://msdn.microsoft.com/en-us/library/ms175046(v=sql.105).aspx
3. http://msdn.microsoft.com/en-us/library/ms175046(v=sql.100).aspx
4. http://msdn.microsoft.com/en-us/library/ms190693(v=sql.110).aspx
5. http://msdn.microsoft.com/en-us/library/ms190693(v=sql.105).aspx
6. http://msdn.microsoft.com/en-us/library/ms190693(v=sql.100).aspx

3.3 Disable the 'xp_dirtree' procedure (Scored)

Profile Applicability:

- Level 1

Description:

Returns a result set of the directory tree for a given directory path.

Rationale:

Ensuring this procedure is disabled will prevent an attacker from performing directory enumeration and listing files and folders to read or write data to\from. This procedure is currently leveraged by several automated SQL Injection tools

Audit:

To view the permissions for this stored procedure, perform the following steps in SQL Server Management Studio:

1. In Object Explorer, navigate to the SQL Server instance and expand the path: `Databases\System Databases\master\Programmability\Extended Stored Procedures`
2. Locate `xp_dirtree`, right click and select Properties.
3. The permissions for this extended stored procedure can be viewed in the Permissions tab.

Remediation:

Revoke use by all general users on the SQL Server machine:

```
REVOKE EXECUTE ON xp_dirtree TO PUBLIC;
```

Note: Server logins within the sysadmin role will retain use of this procedure

3.4 Disable the 'xp_enumgroups' procedure (Scored)

Profile Applicability:

- Level 1

Description:

This procedure provides a list of local Microsoft Windows groups or a list of global groups that are defined in a specified Windows machine.

Rationale:

Ensuring this procedure is disabled will limit an attacker's ability to identify the Windows groups present on teh SQL Server machine. This procedure is currently leveraged by several automated SQL Injection tools

Audit:

To view the permissions for this stored procedure, perform the following steps in SQL Server Management Studio:

1. In Object Explorer, navigate to the SQL Server instance and expand the path: `Databases\System Databases\master\Programmability\Extended Stored Procedures`

2. Locate `xp_enumgroups`, right click and select Properties.
3. The permissions for this extended stored procedure can be viewed in the Permissions tab.

Remediation:

Revoke use by all general users on the SQL Server machine:

```
REVOKE EXECUTE ON xp_enumgroups to PUBLIC;
```

Note: Server logins within the sysadmin role will retain use of this procedure

3.5 Disable the 'xp_fixeddrives' procedure (Scored)

Profile Applicability:

- Level 1

Description:

Returns a list of all hard drives on the machine and the space free in megabytes for each drive

Rationale:

Ensuring this procedure is disabled will prevent an attacker from viewing local available drives for directory and file enumeration.

Audit:

To view the permissions for this stored procedure, perform the following steps in SQL Server Management Studio:

1. In Object Explorer, navigate to the SQL Server instance and expand the path: `Databases\System Databases\master\Programmability\Extended Stored Procedures`
2. Locate `xp_fixeddrives`, right click and select Properties.
3. The permissions for this extended stored procedure can be viewed in the Permissions tab.

Remediation:

Revoke use by all general users on the SQL Server machine:

```
REVOKE EXECUTE ON xp_fixeddrives TO PUBLIC;
```

Note: Server logins within the sysadmin role will retain use of this procedure

3.6 Disable the 'xp_servicecontrol' procedure (Scored)

Profile Applicability:

- Level 1

Description:

Can be used to start and stop windows services running on the SQL Server machine.

Rationale:

Can be used by a remote attacker to shutdown Windows services associated with Anti-virus products or firewalls to loosen the security posture of a database server.

Audit:

To view the permissions for this stored procedure, perform the following steps in SQL Server Management Studio:

1. In Object Explorer, navigate to the SQL Server instance and expand the path: `Databases\System Databases\master\Programmability\Extended Stored Procedures`
2. Locate `xp_servicecontrol`, right click and select Properties.
3. The permissions for this extended stored procedure can be viewed in the Permissions tab.

Remediation:

Revoke use by all general users on the SQL Server machine:

```
REVOKE EXECUTE ON xp_servicecontrol TO PUBLIC;
```

3.7 Disable the 'xp_subdirs' procedure (Scored)

Profile Applicability:

- Level 1

Description:

Lists all subdirectories listed for a given folder path.

Rationale:

Ensuring this procedure is disabled will prevent an attacker from performing directory enumeration and listing all subdirectories on the file system for a given directory path. This is information that an attacker would be able to make use of to determine where key OS files are located.

Audit:

To view the permissions for this stored procedure, perform the following steps in SQL Server Management Studio:

1. In Object Explorer, navigate to the SQL Server instance and expand the path: `Databases\System Databases\master\Programmability\Extended Stored Procedures`
2. Locate `xp_subdirs`, right click and select Properties.
3. The permissions for this extended stored procedure can be viewed in the Permissions tab.

Remediation:

Revoke use by all general users on the SQL Server machine:

```
REVOKE EXECUTE ON xp_subdirs TO PUBLIC;
```

Note: Server logins within the sysadmin role will retain use of this procedure

3.8 Disable the 'xp_regaddmultistring' procedure (Scored)

Profile Applicability:

- Level 1

Description:

Adds multiple strings to the server's registry.

Rationale:

Ensuring this procedure is disabled will prevent a SQL Server user from writing to the Windows registry via SQL Server.

Audit:

To view the permissions for this stored procedure, perform the following steps in SQL Server Management Studio:

1. In Object Explorer, navigate to the SQL Server instance and expand the path: `Databases\System Databases\master\Programmability\Extended Stored Procedures`
2. Locate `xp_regaddmultistring`, right click and select Properties.
3. The permissions for this extended stored procedure can be viewed in the Permissions tab.

Remediation:

Revoke use by all general users on the SQL Server machine:

```
REVOKE EXECUTE ON xp_regaddmultistring TO PUBLIC;
```

Note: Server logins within the sysadmin role will retain use of this procedure

3.9 Disable the 'xp_regdeletekey' procedure (Scored)

Profile Applicability:

- Level 1

Description:

Deletes registry keys from the server's registry

Rationale:

Ensuring this procedure is disabled will prevent a SQL Server user from deleting values from the Windows registry via SQL Server.

Audit:

To view the permissions for this stored procedure, perform the following steps in SQL Server Management Studio:

1. In Object Explorer, navigate to the SQL Server instance and expand the path: `Databases\System Databases\master\Programmability\Extended Stored Procedures`
2. Locate `xp_regdeletekey`, right click and select Properties.
3. The permissions for this extended stored procedure can be viewed in the Permissions tab.

Remediation:

Revoke use by all general users on the SQL Server machine:

```
REVOKE EXECUTE ON xp_regdeletekey TO PUBLIC;
```

Note: Server logins within the sysadmin role will retain use of this procedure

3.10 Disable the 'xp_regdeletevalue' procedure (Scored)

Profile Applicability:

- Level 1

Description:

Deletes values from the server's registry.

Rationale:

Ensuring this procedure is disabled will prevent a SQL Server user from deleting values from the Windows registry via SQL Server.

Audit:

To view the permissions for this stored procedure, perform the following steps in SQL Server Management Studio:

1. In Object Explorer, navigate to the SQL Server instance and expand the path: `Databases\System Databases\master\Programmability\Extended Stored Procedures`
2. Locate `xp_regdeletevalue`, right click and select Properties.
3. The permissions for this extended stored procedure can be viewed in the Permissions tab.

Remediation:

Revoke use by all general users on the SQL Server machine:

```
REVOKE EXECUTE ON xp_regdeletevalue TO PUBLIC;
```

Note: Server logins within the sysadmin role will retain use of this procedure

3.11 Disable the 'xp_regenumvalues' procedure (Scored)

Profile Applicability:

- Level 1

Description:

Enumerates a set of values from a provided registry path.

Rationale:

Ensuring this procedure is disabled will prevent a SQL Server user from enumerating and reading registry values.

Audit:

To view the permissions for this stored procedure, perform the following steps in SQL Server Management Studio:

1. In Object Explorer, navigate to the SQL Server instance and expand the path: `Databases\System Databases\master\Programmability\Extended Stored Procedures`
2. Locate `xp_regenumvalues`, right click and select Properties.
3. The permissions for this extended stored procedure can be viewed in the Permissions tab.

Remediation:

Revoke use by all general users on the SQL Server machine:

```
REVOKE EXECUTE ON xp_regenumvalues TO PUBLIC;
```

Note: Server logins within the sysadmin role will retain use of this procedure

3.12 Disable the 'xp_regremovemultistring' procedure (Scored)

Profile Applicability:

- Level 1

Description:

Removes multiple strings from the server's registry.

Rationale:

Ensuring this procedure is disabled will prevent a SQL Server user from deleting batch values from the Windows registry via SQL Server.

Audit:

To view the permissions for this stored procedure, perform the following steps in SQL Server Management Studio:

1. In Object Explorer, navigate to the SQL Server instance and expand the path: `Databases\System Databases\master\Programmability\Extended Stored Procedures`
2. Locate `xp_regremovemultistring`, right click and select Properties.
3. The permissions for this extended stored procedure can be viewed in the Permissions tab.

Remediation:

Revoke use by all general users on the SQL Server machine:

```
REVOKE EXECUTE ON xp_regremovemultistring TO PUBLIC;
```

Note: Server logins within the sysadmin role will retain use of this procedure

3.13 Disable the 'xp_regwrite' procedure (Scored)

Profile Applicability:

- Level 1

Description:

Writes key values to the server's registry.

Rationale:

Ensuring this procedure is disabled will prevent a SQL Server user from writing to the Windows registry via SQL Server.

Audit:

To view the permissions for this stored procedure, perform the following steps in SQL Server Management Studio:

1. In Object Explorer, navigate to the SQL Server instance and expand the path: `Databases\System Databases\master\Programmability\Extended Stored Procedures`
2. Locate `xp_regwrite`, right click and select Properties.
3. The permissions for this extended stored procedure can be viewed in the Permissions tab.

Remediation:

Revoke use by all general users on the SQL Server machine:

```
REVOKE EXECUTE ON xp_regwrite TO PUBLIC;
```

Note: Server logins within the sysadmin role will retain use of this procedure

3.14 Disable the 'xp_regread' procedure (Scored)

Profile Applicability:

- Level 1

Description:

Reads key values from the server's registry.

Rationale:

Ensuring this procedure is disabled will prevent a SQL Server user from enumerating and reading registry values. This procedure is leveraged by several automated SQL injection tools.

Audit:

To view the permissions for this stored procedure, perform the following steps in SQL Server Management Studio:

1. In Object Explorer, navigate to the SQL Server instance and expand the path: `Databases\System Databases\master\Programmability\Extended Stored Procedures`
2. Locate `xp_regread`, right click and select Properties.
3. The permissions for this extended stored procedure can be viewed in the Permissions tab.

Remediation:

Revoke use by all general users on the SQL Server machine:

```
REVOKE EXECUTE ON xp_regread TO PUBLIC;
```

Note: Server logins within the sysadmin role will retain use of this procedure

4 Authentication and Authorization

[This space intentionally left blank]

4.1 Set The 'Server Authentication' Property To Windows Authentication mode (Not Scored)

Profile Applicability:

- Level 1

Description:

Uses Windows Authentication to validate attempted connections

Rationale:

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

Audit:

Execute the followin 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.

References:

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

4.2 Revoke CONNECT permissions on the 'guest user' within all SQL Server databases excluding the master, msdb and tempdb (Scored)

Profile Applicability:

- Level 1

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 exists.

```
SELECT DB_NAME(), name
FROM sys.database_principals
WHERE name = 'guest'
```

Remediation:

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

```
REVOKE CONNECT FROM guest;
```

Impact:

Default Value:
The guest user account is added to each new database by default.

References:
http://msdn.microsoft.com/en-us/library/bb402861%28v=sql.100%29.aspx

References:

1. http://msdn.microsoft.com/en-us/library/bb402861%28v=sql.100%29.aspx

4.3 Drop Oprhaned Users From SQL Server Databases (Scored)

Profile Applicability:

- Level 1

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 remove an orphan user:

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

Remediation:

Run the following T-SQL query to identify orphan users:

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

5 Password Policy

Password policy settings

5.1 Set the 'MUST_CHANGE' Option To ON For All SQL Authenticated Logins (Not Scored)

Profile Applicability:

- Level 1

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 cahnge 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

References:

1. http://technet.microsoft.com/en-us/library/ms189828.aspx

5.2 Set the 'CHECK_EXPIRATION' Option to ON For All SQL Authenticated Logins Within the Sysadmin Role (Scored)

Profile Applicability:

- Level 1

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:

```
SELECT SQLLoginName = sp.name,  PasswordExpirationEnforced =
CAST(sl.is_expiration_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';
```

Remediation:

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

References:

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

5.3 Set the 'CHECK_POLICY' Option To ON For All SQL Authenticated Logins (Scored)

Profile Applicability:

- Level 1

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 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;
```

References:

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

6 Auditing and Logging

TODO: Pair SQL Trace and SQL Audit events; break them into two parts, level 1 and 2.

6.1 Set the 'Maximum number of error log files' setting to 12 (Not Scored)

Profile Applicability:

- Level 1

Description:

SQL Server errorlog files must be protected from loss. The log files must be backed up before they are overwritten.

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 12

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 12

References:

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

6.2 Set the 'Default Trace Enabled' Server Configuration Option to 1 (Scored)

Profile Applicability:

- Level 1

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;
```

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

6.3 Set 'Login Auditing' to Both failed and successful logins (Not Scored)

Profile Applicability:

- Level 1

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 a 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.

References:

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

7 Application Development

[This space intentionally left blank]

7.1 Sanitize Database and Application User Input (Not Scored)

Profile Applicability:

- Level 1
- Level 2

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 applicaiton 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. http://msdn.microsoft.com/en-us/library/ms161953%28v=SQL.100%29.aspx
2. https://www.owasp.org/index.php/SQL_Injection

7.2 Set the 'CLR Assembly Permission Set' to SAFE_ACCESS For All CLR Assemblies (Scored)

Profile Applicability:

- Level 1
- Level 2

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.

Audit:

Run the following T-SQL query:

1. 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 = EXTERNAL_ACCESS
```

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.

References:

1. http://msdn.microsoft.com/en-us/library/ms345101(v=sql.105).aspx

Appendix: Change History

Date	Version	Changes for this version
11-15-2012	1.0.0	Initial release.