

Report for:

Database Review Security Assessment Sample Report

ClientName

March 19, 2021

Version: 3.0

Prepared by: NCC Consultant

Email: n.consultant@nccgroup.com

Telephone: +44 (0)161 209 5200



Assured Service Provider



in association with
**National Cyber
Security Centre**



NCC Group PLC - Security Testing Audit and Compliance

XYZ Building,
2 Hardman Boulevard,
Spinningfields,
Manchester,
M3 3AQ
<https://www.nccgroup.com>

1 Executive Summary

This report presents the findings of the Database Review Security Assessment conducted on behalf of Client Company Ltd (ClientName). The assessment was conducted between 08/03/2021 and 12/03/2021 and was authorised by ClientName.

The system being assessed was a pair of business-critical databases containing sensitive data.

1.1 Overview

The issues identified could allow an attacker who had managed to access the internal network on which these databases were located to potentially gain access to the databases and the information they contained. As these databases were analytic sandboxes containing large volumes of collated sales, pricing and customer demographic data, this information is of considerable commercial sensitivity. A significant data breach could materially affect ClientName's performance.

The following table breaks down the issues which were identified by component and severity of risk (issues which are reported for information only are not included in the totals):

Component	Critical	High	Medium	Low	Total
Phase 1 –Oracle Database Assessment	1	3	4	1	9
Phase 2 –SQL Server Database Assessment	0	1	7	2	10
Total	1	4	11	3	19

1.2 Assessment Summary

This assessment reviewed instances of both the Oracle and SQL Server databases used by ClientName. Both database types were affected by issues that could allow an attacker who was able to access the internal network to authenticate to these databases and access the commercially sensitive information held within them. The Oracle database was assessed to expose ClientName to a greater degree of risk than the SQL Server database due to the presence of one critical and three high risk issues.

The critical risk issue, associated only with the Oracle database, was the absence of a substantial number of security updates, some rated as Critical or High by the vendor. This resulted in the database being vulnerable to a number of publicly documented security issues that could be exploited by an attacker.

Another area of concern was associated with the protection of user credentials. This affected both types of database. A number of issues were identified, with the most significant assessed to pose a high risk. These issues could allow an attacker to identify valid credentials and hence authenticate to the database. For example, the Oracle database contained a large number of default passwords for some of the standard accounts provided with the database. An attacker using these default credentials would be able to access some of the database functionality. Similarly, an issue in the SQL server database could allow an attacker to access the encrypted passwords for the database. Should they be able to recover the plaintext equivalents for those passwords, they would be able to authenticate to the database.

Another set of issues was concerned with the security of data in transit. A high risk issue associated with the Oracle database was the ability to carry out an attack called 'TNS Listener Poisoning'. This could, for example, allow a suitably positioned attacker to mirror the nightly flow of commercially sensitive data to the Oracle database and store a copy on a server under the attacker's control. Similarly, it was possible to remotely access the SQL Server database from other SQL servers. An attacker able to compromise a remote SQL Server database could use it to gain access to the sensitive information held on the SQL Server database in scope.

Finally, a number of configuration options used default or insecure settings. For example, C2 auditing was not enabled in the SQL Server database. This logs attempts to access objects in the database and is useful in tracking unexpected activity or potential security violations in the database.

The remaining issues were all assessed to pose a low risk. More detailed information on each of the issues which were identified is included in the Technical Details section of this report.

1.3 Strategic Recommendations

The most significant issue was assessed to pose a critical risk and arose because of the failure to apply security updates to the Oracle database in a timely manner. It is therefore recommended that, in addition to addressing the individual issues which are set out in this report, the ClientName's patching policy and procedures should also be reviewed to ensure that these issues do not recur once the individual instances documented here have been addressed.

The assessment identified the presence of a number of ways an attacker could potentially identify valid user credentials for both the Oracle and SQL Server databases. Once in possession of these credentials and attacker would be able to access (and potentially exfiltrate) the commercially sensitive information held in these databases. It is therefore recommended that the organisation-wide password policy should be reviewed. It should also be ensured that this policy is enforced consistently across all the systems within the organisation's information estate.

Finally, a number of configuration options in both databases did not appear to have been security hardened beyond the default settings or were not configured in the most secure manner. Default settings are rarely the most secure and it is therefore recommended that the guidelines published by the vendor for this security hardening of this platform be followed.

It is recommended that the issues set out in this report should be addressed by a structured programme of remedial actions which is prioritised by the risk perceived by ClientName. This should bring the database configuration into line with security best practice. It is important to recognise that even low risk issues can be exploited in combination with other issues as part of a wider attack which seeks to compromise an environment or application. In addition, resolving lower risk issues can have the dual benefit of reducing the attractiveness of systems to opportunistic attackers as well as enhancing the overall security posture.

Finally, it is recommended that any configuration changes which are made as a result of this report are also considered for inclusion in the organisation's build standards and secure deployment procedures. This will help to ensure that similar issues do not recur and so maintain the organisation's security posture at an appropriate level.

2 Table of Contents

1	Executive Summary	2
1.1	Overview	2
1.2	Assessment Summary	2
1.3	Strategic Recommendations	3
2	Table of Contents	4
3	Technical Summary	5
3.1	Scope	5
3.2	Caveats	5
3.3	Post Assessment Cleanup	5
3.4	Risk Ratings	6
3.5	Findings Overview	7
4	Technical Details	9
4.1	Phase 1 –Oracle Database Assessment	9
4.2	Phase 2 –SQL Server Database Assessment	18
5	Supplemental Data - Missing Oracle Security Patches.....	28
6	Supplemental Data - Excessive Users with Default Profile	29
7	Document Control	31
7.1	Document Data	31
7.2	Document History	31
7.3	Document Distribution List	31
8	Assessment Team	32

3 Technical Summary

NCC Group was contracted by ClientName to conduct a security assessment of the systems within scope in order to identify security issues that could negatively affect ClientName's business or reputation if they led to the compromise or abuse of systems.

3.1 Scope

The security assessment was carried out in the live environment and included:

- ◆ Assessment of Oracle Database
- ◆ Assessment of SQL Server Database

The IP addresses and hostnames within the scope of this test are listed below:

- ◆ 192.168.4.3 / ORADB
- ◆ 192.168.3.1 / MSSQLDB

3.2 Caveats

The authorisation forms giving permission for NCC Group to test the databases were not received until 11 o'clock on the first day of testing, leading to the loss of several hours of testing time. Despite this, good coverage was achieved and the delay in obtaining these forms is not thought to have materially affected the quality of the testing.

Due to the nature of the environment, checks that would have a high probability of causing disruption to the named hosts were excluded. Denial of service attempts were excluded for the same reason.







3.3 Post Assessment Cleanup

Any test accounts which were created for the purpose of this assessment should be disabled or removed, as appropriate, together with any associated content.

Revert any WAF/IDS/IPS/firewall changes which were made for the purposes of the assessment.

3.4 Risk Ratings










The table below gives a key to the icons and symbols used throughout this report to provide a clear and concise risk scoring system. It should be stressed that quantifying the overall business risk posed by any of the issues found in any test is outside our remit. This means that some risks may be reported as high from a technical perspective but may, as a result of other controls unknown to us, be considered acceptable.

Symbol	Risk Rating	CVSSv2 Score	Explanation
	CRITICAL	9.0 - 10	A vulnerability was discovered that has been rated as critical. This requires resolution as quickly as possible.
	HIGH	7.0 - 8.9	A vulnerability was discovered that has been rated as high. This requires resolution in the short term.
	MEDIUM	4.0 - 6.9	A vulnerability was discovered that has been rated as medium. This should be resolved as part of the ongoing security maintenance of the system.
	LOW	1.0 - 3.9	A vulnerability was discovered that has been rated as low. This should be addressed as part of routine maintenance tasks.
	INFO	0 - 0.9	A discovery was made that is reported for information. This should be addressed in order to meet leading practice.
	GOOD	N/A	Good security practices were being followed or an audit item was found to be present and correct.


3.5 Findings Overview










All the issues identified during the assessment are listed below with a risk rating for each issue.

Phase 1 –Oracle Database Assessment

Ref	Finding	Risk
SR-103-001	Missing Oracle Security Patches	Critical 
SR-103-002	Oracle TNS Listener Poisoning Attack	High 
SR-103-003	Default Passwords	High 
SR-103-004	Remote Login Password File in Use	High 
SR-103-005	Default Profile Settings Not Configured	Medium 
SR-103-006	Case Insensitive Password Hashes in Use	Medium 
SR-103-007	Users With CREATE PROCEDURE Privilege	Medium 
SR-103-008	Database Communication Over Clear Text	Medium 
SR-103-010	Excessive Users With Default Profile	Low 


Phase 2 –SQL Server Database Assessment

Ref	Finding	Risk
SR-103-011	SQL Server Running As Local System	High 

Ref	Finding	Risk
SR-103-012	C2 Audit Not Configured	Medium 
SR-103-013	xp_cmdshell Enabled	Medium 
SR-103-014	Default "sa" Administrator Account Configured	Medium 
SR-103-015	Enforce Password Expiration Not Set	Medium 
SR-103-016	Mixed Mode Authentication	Medium 
SR-103-017	PUBLIC Role Permissions on xp_instance_regread and xp_regread Stored Procedures	Medium 
SR-103-018	Remote Access via RPC	Medium 
SR-103-019	Login Auditing Failed Logins Only	Low 
SR-103-020	Number of Error Logs is Too Low	Low 

4 Technical Details

4.1 Phase 1 –Oracle Database Assessment

SR-103-001	Missing Oracle Security Patches	
Risk Rating	Critical	Status Open

Description:

The Oracle database management system was found to be missing multiple security patches, leaving it vulnerable to the possibility that an attacker may gain access, escalate their privileges, or cause a denial of service attack on the database software.

Oracle release a quarterly critical patch update, known as a CPU. These updates contain a selection of critical patches which affect the system, as well as security updates. The server was found to be missing the following CPUs:

- ◆ January 2021 CPU
- ◆ October 2020 CPU
- ◆ July 2020 CPU
- ◆ April 2020CPU
- ◆ January 2020 CPU
- ◆ October 2019 CPU
- ◆ July 2019 CPU
- ◆ January 2019 CPU
- ◆ October 2018 CPU

Only the most recent missing CPUs are listed above. For the complete list of missing patches refer to Supplemental Data - Missing Oracle Security Patches on page 28.

Recommendation:

It is strongly recommended that the database is patched to a later CPU that will fix the majority of known issues.¹

A patching policy should be put in place that assesses any new patches for risk.

Affects:

IP Address	DNS Name	Instance
192.168.4.3	ORADB	SAMPLE

¹Critical Patch Updates, Security Alerts and Third Party Bulletin by Oracle <https://www.oracle.com/technetwork/topics/security/alerts-086861.html>

SR-103-002 Oracle TNS Listener Poisoning Attack



Risk Rating

High

Status

Open

Description:

The Oracle TNS listener running on the server permitted service registration from remote hosts. An anonymous attacker able to connect to the listener could permit a poisoning attack, which would enable the attacker to manipulate database instances, potentially facilitating man-in-the-middle, session-hijacking, or denial of service attacks against the server.

An attacker would be able to register new services and instances. By specifying the name of a legitimate instance, the TNS listener can be convinced that the attacker's new instance is actually a failover or cluster participant for the legitimate instance. This can enable the redirection of legitimate client connections to an attacker-controlled machine.

Recommendation:

Apply the Oracle Critical Patch Update (CPU) from April 2012.^{2,3}

If this is not possible, apply the Class of Secure Transport (COST) workaround specified in the Oracle advisory references listed below.

Affects:

IP Address	DNS Name	Instance
192.168.4.3	ORADB	SAMPLE

²Oracle Security Alert for CVE-2012-1675 <https://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html>

³The history of a -probably- 13 years old Oracle bug: TNS Poison <https://seclists.org/fulldisclosure/2012/Apr/204>



SR-103-003

Default Passwords



Risk Rating

High

Status

Open

Description:

Several user accounts were found to have default passwords.

The affected accounts are listed below:

- | | |
|--------------|--------------|
| ◆ ABM | ◆ ODM_MTR |
| ◆ AD_MONITOR | ◆ OKB |
| ◆ AHM | ◆ OKO |
| ◆ AMF | ◆ OKR |
| ◆ APPLSYSPUB | ◆ OLAPSYS |
| ◆ APPQOSSYS | ◆ ORACLE_OCM |
| ◆ CSS | ◆ ORDDATA |
| ◆ CTXSYS | ◆ ORDPLUGINS |
| ◆ CUE | ◆ ORDSYS |
| ◆ CUN | ◆ OUTLN |
| ◆ DBSNMP | ◆ OWAPUB |
| ◆ DIP | ◆ OZS |
| ◆ DMSYS | ◆ RHX |
| ◆ EAA | ◆ SCOTT |
| ◆ EVM | ◆ SSOSDK |
| ◆ FPT | ◆ SYS |
| ◆ IBA | ◆ VEH |
| ◆ IPD | ◆ XDB |
| ◆ MDDATD | ◆ XNC |
| ◆ MDSYS | ◆ XNI |
| ◆ ME | ◆ XNM |
| ◆ MGDSYS | ◆ XNS |
| ◆ ODM | |

Some of these accounts are privileged accounts and should have been configured with strong passwords.

Recommendation:

It is recommended to change the passwords for these accounts. Default passwords allow attackers access to the database without triggering any alarms since brute-force attacks are not required.⁴

New strong passwords should be set in line with the company password policy.

Affects:

IP Address	DNS Name	Instance
192.168.4.3	ORADB	SAMPLE

⁴Securing Oracle Database User Accounts https://docs.oracle.com/cd/E11882_01/server.112/e10575/tdpsg_user_accounts.htm#TDPSG20000



SR-103-004 Remote Login Password File in Use



Risk Rating

High

Status

Open

Description:

The remote login password file had not been disabled.

Remote users can authenticate to the database using the INTERNAL account, or SYSDBA and SYSOPER modes. Using this method the users' password hashes are held in the Remote Login Password file. This file is named orapw[SID] on Unix platforms. Controls on failed login attempts cannot prevent brute-force attacks on hashes in this file, nor is auditing access possible under Oracle. It is recommended that this feature is disabled and alternative methods used for remote database connection. Setting this parameter to NONE will enforce OS authenticated connections as SYSDBA. The roles OSDBA and OSOPER also exist to allow OS authenticated users to connect to the database with system level privileges.

The parameter was set to EXCLUSIVE which means that only one database can use the file, however this setting did not add any security at the database configuration.

Recommendation:

This feature should be disabled by setting remote_login_passwordfile to NONE in the init.ora file.⁵

Affects:

IP Address	DNS Name	Instance
192.168.4.3	ORADB	SAMPLE

⁵Remote login password file https://docs.oracle.com/cd/B28359_01/server.111/b28320/initparams198.htm#REFRN10184

SR-103-005

Default Profile Settings Not Configured



Risk Rating

Medium

Status

Open

Description:

The default profile was found not to be configured and password related parameters were set to default values.

The following parameters were not configured:

- ◆ PASSWORD_GRACE_TIME
- ◆ PASSWORD_LOCK_TIME
- ◆ PASSWORD_VERIFY_FUNCTION
- ◆ PASSWORD_REUSE_MAX
- ◆ PASSWORD_REUSE_TIME
- ◆ PASSWORD_LIFE_TIME
- ◆ FAILED_LOGIN_ATTEMPTS

All values were set to unlimited or null. Therefore all user accounts under the Default role were vulnerable to password guessing attacks, since there was no timeout or other restrictions in place regarding password use.

Recommendation:

All the parameters mentioned above should be configured according to company password policies and the criticality of the database.⁶

Affects:

IP Address	DNS Name	Instance
192.168.4.3	ORADB	SAMPLE

⁶Managing User Privileges https://docs.oracle.com/cd/E11882_01/server.112/e10575/tdpsg_privileges.htm#TDP3G30038



SR-103-006 Case Insensitive Password Hashes in Use



Risk Rating

Medium

Status

Open

Description:

A number of Oracle users had case-insensitive password hashes. These older style password hashes are easily crackable, making them insecure.

The highlighted password below is an example of a user with case-insensitive password:

```
SQL> select name, password, spare4 from sys.user$;
NAME      PASSWORD      SPARE4
SYS       CXXXXXXXXXXXX9  S:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX3
```

Note that the SEC_CASE_SENSITIVE_LOGON parameter had been set to true meaning that all new users will not have a case-insensitive password. Only existing users will continue to have this older style hash until the hash is removed.

Recommendation:

Remove the weak hash manually for each account where this is set using the following command:⁷

```
UPDATE SYS.USER$ SET password = '' WHERE name = [USER]
```

Additionally, it is recommended that the users' passwords be changed. If they are not changed and the weaker hashes are cracked then this would reveal the users' password regardless of whether they were using the new hash.

Affects:

IP Address	DNS Name	Instance
192.168.4.3	ORADB	SAMPLE

⁷Oracle Password Hashes <https://marcel.vandewaters.nl/oracle/security/password-hashes>



SR-103-007
Users With CREATE PROCEDURE Privilege

Risk Rating

Medium

Status

Open

Description:

A number of user roles had been assigned the CREATE PROCEDURE system privilege. Having the ability to create procedures or functions allows attackers to produce scripts to take advantage of any PL/SQL vulnerabilities that may exist in the database server.

The ability to create procedure or functions allows an attacker to write and execute a recursive loop that will deny service. It is suggested that this privilege be dropped from the RESOURCE role and another role should be created and assigned the CREATE PROCEDURE privilege.

```
APEX_030200
AUDIT_PARTITION_MAINT
ASSET_SCHEMA
AUDIT_MAINTENANCE
RESOURCE
```

Recommendation:

Assign this role only to those users that must, as a strict business requirement, be able to create procedures or functions.

Affects:

IP Address	DNS Name	Instance
192.168.4.3	ORADB	SAMPLE

SR-103-008
Database Communication Over Clear Text

Risk Rating

Medium

Status

Open

Description:

A number of listener connections were identified to allow clear text communication. If an attacker has access to the network and is able to sniff the network traffic then the confidentiality and integrity of this transmission could be affected.

The following listeners were identified in the tnsnames.ora file as allowing clear text communication:

SAMPLE	SERVICE_NAME=SAMPLE . SAMPLE . co . uk
--------	--

Within each of these listeners the following had been set:

PROTOCOL = TCP

Having the protocol set to TCP states that encryption should not be utilised.

Recommendation:

The TCPS protocol should be specified for each listener within the tnsnames.ora configuration file.

An example of how the listener should be configured is shown below:

PROTOCOL = TCPS

Affects:

IP Address	DNS Name	Instance
192.168.4.3	ORADB	SAMPLE

SR-103-010 Excessive Users With Default Profile**Risk Rating**

Low

Status

Open

Description:

During the assessment 258 users were found to be using the default profile.

The Oracle default profile is very permissive in terms of password requirements and access control. The large number of users with this profile are therefore exposed to heightened risk of account compromise.

For the complete users list refer to Supplemental Data - Excessive Users with Default Profile on page 29.

Recommendation:

It is recommended to create different profiles according to the different tasks each user is performing on the database.⁸


Affects:

IP Address	DNS Name	Instance
192.168.4.3	ORADB	SAMPLE

⁸**Managing User Privileges** https://docs.oracle.com/cd/E11882_01/server.112/e10575/tdpsg_privileges.htm#TDP3G30038



4.2 Phase 2 –SQL Server Database Assessment

SR-103-011	SQL Server Running As Local System	
Risk Rating	High	Status Open

Description:

The SQL Server service was running in the context of the Local System account on the host. This means that should any vulnerability be discovered in the database, allowing an attacker to access xp_cmdshell, then they would be able to run commands as Local System and would have gained full access to the underlying host. The Local System account has permission to access the SAM database in the Windows registry. The SAM database contains the password hashes of all users of the system, and tools exist that can recover the plaintext passwords from these hashes.

Recommendation:

The database should be installed as a lower privileged domain user, rather than as Local System.⁹

Affects:

IP Address	DNS Name	Instance
192.168.3.1	MSSQLDB	SAMPLE

⁹**LocalSystem Account** [https://msdn.microsoft.com/en-us/library/windows/desktop/ms684190\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms684190(v=vs.85).aspx)

SR-103-012 C2 Audit Not Configured



Risk Rating

Medium

Status

Open

Description:

C2 audit was not configured (via sp_configure). C2 audit mode allows auditing of attempts, both successful and unsuccessful, to access objects. It also ensures that the server will automatically shut down if it is unable to log an event (although this may not be desirable in every organisation).

Recommendation:

Consider configuring C2 audit mode, using the following commands:¹⁰

```
exec sp_configure 'show advanced options', '1'; reconfigure with override
exec sp_configure 'c2 audit mode', '1'; reconfigure with override
exec sp_configure 'show advanced options', '0'; reconfigure with override
```

Affects:

IP Address	DNS Name	Instance
192.168.3.1	MSSQLDB	SAMPLE

¹⁰What is C2 Audit Tracing in SQL Server <https://appliedsql.net/2013/11/28/what-is-c2-audit-tracing-in-sql-server/>

SR-103-013 xp_cmdshell Enabled



Risk Rating

Medium

Status

Open

Description:

The execution of the extended stored procedure `xp_cmdshell` was enabled on the system (this is disabled by default). This allows users who are granted execute permission on this stored procedure to directly run operating system commands. This should always be disabled unless required for backwards compatibility.

The following screenshot shows the result of the query `select name, value_in_use from sys.configurations where name = 'xp_cmdshell'` and `value_in_use = 1`, indicating that `xp_cmdshell` was enabled.

Recommendation:

The `xp_cmdshell` stored procedure should be disabled, and ideally removed from the database.¹¹

Affects:

IP Address	DNS Name	Instance
192.168.3.1	MSSQLDB	SAMPLE

¹¹`xp_cmdshell` <https://docs.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/xp-cmdshell-transact-sql>



SR-103-014

Default "sa" Administrator Account Configured

**Risk Rating**

Medium

Status

Open

Description:

The SQL Server administrator account had not been renamed from the default of 'sa'. It is more difficult to script attacks against the administrator account if the username is not known. This account should be renamed to a value other than the default.

Recommendation:

The code below will disable and rename the sa account:¹²

```
ALTER LOGIN sa DISABLE;  
ALTER LOGIN sa WITH NAME = Admin_User;
```

Affects:

IP Address	DNS Name	Instance
192.168.3.1	MSSQLDB	SAMPLE

¹²Microsoft SQL Server - Choose an Authentication Mode <https://msdn.microsoft.com/en-us/library/ms144284.aspx>

SR-103-015 Enforce Password Expiration Not Set



Risk Rating

Medium

Status

Open

Description:

A number of accounts were found to lack the 'Enforce Password Expiration' flag, allowing the use of the same password for extended periods, which may lead to the accounts being compromised.

Instance: SAMPLE

Name	Expiration Checked
------	--------------------

User1	No
-------	----

Admin1	No
--------	----

Sa	No
----	----

Recommendation:

It is recommended to enforce the use of password expiry on all accounts, to ensure that passwords are changed on a regular basis. This can be achieved in SQL Server Management Studio by selecting an account's properties and checking the box 'Enforce Password Expiration'.

Affects:

IP Address	DNS Name	Instance
------------	----------	----------

192.168.3.1	MSSQLDB	SAMPLE
-------------	---------	--------

SR-103-016
Mixed Mode Authentication

Risk Rating

Medium

Status

Open

Description:

SQL Server was configured to run in mixed mode, which allowed clients to authenticate using either integrated Windows or native SQL Server methods. Using native authentication means that passwords are passed across the network in a form that can easily be decrypted.

Recommendation:


The server should be configured to use Windows authentication only.¹³

Affects:

IP Address	DNS Name	Instance
192.168.3.1	MSSQLDB	SAMPLE

¹³Microsoft - Change Server Authentication Mode <https://technet.microsoft.com/en-us/library/ms188670.aspx>



SR-103-017	PUBLIC Role Permissions on xp_instance_regread and xp_regread Stored Procedures	
Risk Rating	Medium	Status Open

Description:

The PUBLIC role was found to have permission to execute the xp_instance_regread and xp_regread stored procedures. This could lead to compromise of passwords, hashes, or other sensitive information stored in the registry.

Recommendation:

It is recommended to revoke this privilege from the PUBLIC role. The following SQL statements can be used to fix this issue:

```
use master revoke execute on xp_instance_regread to public
use master revoke execute on xp_regread to public
```

Affects:

IP Address	DNS Name	Instance
192.168.3.1	MSSQLDB	SAMPLE

SR-103-018 Remote Access via RPC



Risk Rating

Medium

Status

Open

Description:

It was possible for other SQL Servers to connect to this server over RPC. By default, remote access should not be allowed. Ensure that this is a valid setting for the database and revoke if necessary using sp_configure.

Recommendation:

sp_configure may be used to display or change server-level settings such as this. The following SQL can be used to address this issue:

```
exec sp_configure 'remote access', '0'; reconfigure with override
```

Affects:

IP Address	DNS Name	Instance
192.168.3.1	MSSQLDB	SAMPLE

SR-103-019 Login Auditing Failed Logins Only



Risk Rating

Low

Status

Open

Description:

The login audit settings were only found to log failed logins. Without tracking successful logins it is difficult to track access to the system in the event of a security breach, making forensic analysis harder.

The audit settings were configured as follows:

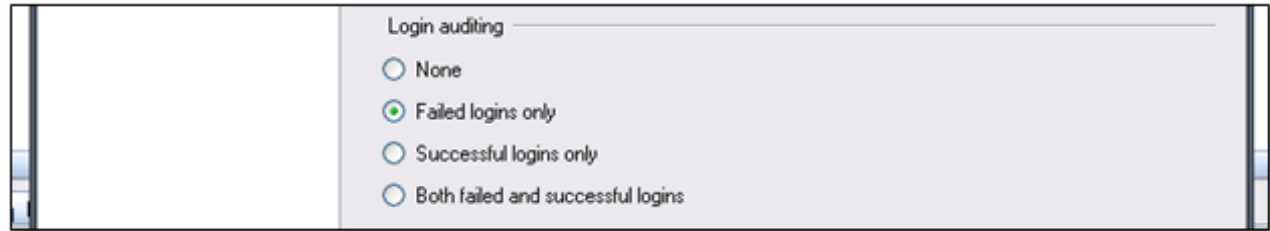


Figure 1: Login Auditing Configuration

Recommendation:

It is recommended to configure auditing to log 'Both failed and successful logins'.

Affects:

IP Address	DNS Name	Instance
192.168.3.1	MSSQLDB	SAMPLE

SR-103-020 Number of Error Logs is Too Low



Risk Rating

Low

Status

Open

Description:

The number of SQL Server error logs that could be created was too low. When this number is reached, old logs will be overwritten.

The value at the time of the assessment was six, the default setting.

Recommendation:

It is recommended that the value be increased to 100 by setting the registry key `HKLM\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer` value `NumErrorLogs` to 100.

Affects:

IP Address	DNS Name	Instance
192.168.3.1	MSSQLDB	SAMPLE

5 Supplemental Data - Missing Oracle Security Patches

◆ Missing Oracle Security Patches

CPU	Description
Redacted	Redacted

6 Supplemental Data - Excessive Users with Default Profile

Complete list of users with Default profile:

Username

Redacted

Username

7 Document Control

Client Confidentiality

This document contains Client Confidential information and may not be copied without written permission.

Proprietary Information

The content of this document should be considered proprietary information and should not be disclosed outside of Client Company Ltd (ClientName).

NCC Group gives permission to copy this report for the purposes of disseminating information within your organisation or any regulatory agency.

7.1 Document Data

Data Classification	Client Confidential
Client Name	ClientName
Project Reference	99999
Proposal Reference	P99999-Sample
Document Title	Database Review Security Assessment Sample Report
Author	NCC Consultant

7.2 Document History

Issue No.	Issue Date	Issued by	Change Description
0.1	2018-01-15	NCC Consultant	Draft for NCC Group internal review only
0.2	2018-01-16	A Reviewer	Revised QA
1.0	2018-01-16	NCC Consultant	Released to client
2.0	2018-02-14	NCC Consultant	Cover page address updated
3.0	2021-03-19	NCC Consultant	Minor content and format changes

7.3 Document Distribution List

Name	Role
A Sponsor	Project Sponsor, ClientName
NCC Consultant	Senior Security Consultant, NCC Group
A Manager	Account Manager, NCC Group

8 Assessment Team

The following members of staff were assigned to this assessment:

Name	Job Title	Comments
NCC Consultant	Senior Security Consultant, NCC Group	CREST Registered Tester (CRT)