secure auditor

Audit Report

Vulnerability Details and Their Solutions

Report Generated Time: 10/13/2011 At 5:57:01PM

Audit Name: : SQLServerAudit(Oct 13 2011 5:56PM)
Description: : Sql Server Audit Report
IP Count : 1
IP(s): : 192.168.100.40

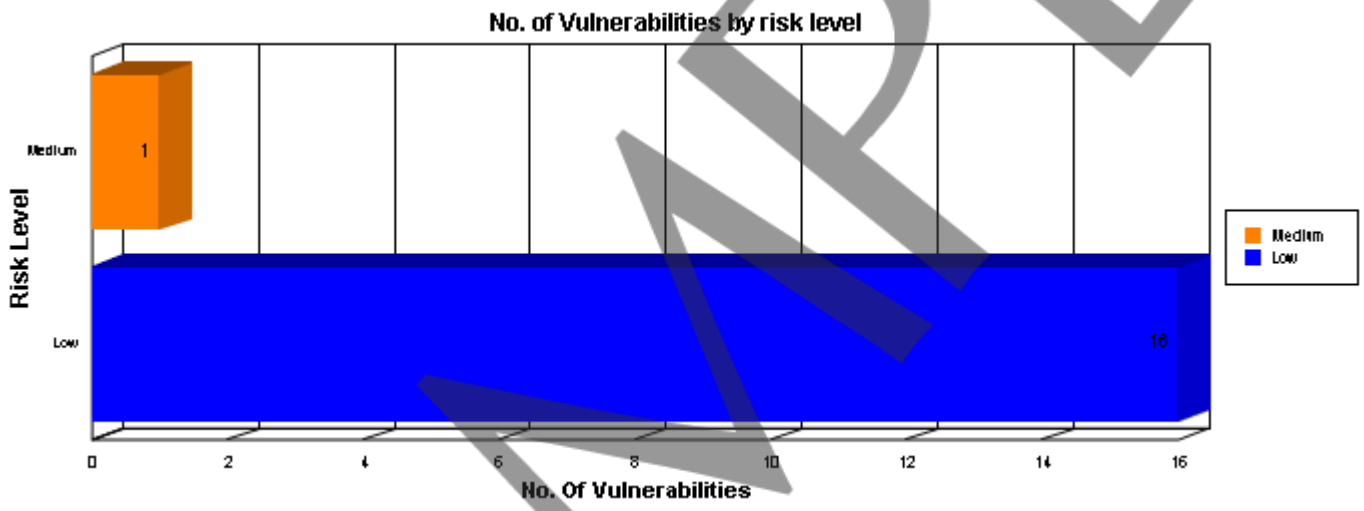
Licensed To : Support
Company Name : Secure Bytes

SECURE BYTES

Vulnerability Details and Their Solutions

Report generated on 13-Oct-2011 At 5:57:01PM

SQL databases are precious ornaments for an organization as most of the information assets are denned there. A security scan was performed on your SQL database or multiple SQL databases.This audit report will give you a complete picture of your database security pasture. This review was performed on your network for single or multiple IP's with their number of audits regarding to single or multiple databases. This Report shows audit detail for each machine and databases name with port numbers. This report is designed to provide a wide-ranging description of vulnerability found on specific audits performed. You can also review the summarized overview of the vulnerabilities discovered. This report covers the maximum researched and checked information about vulnerability including the aspects, ways and areas sensitive or unsafe and usually takes up by attackers. It is recommended to take a thorough review of the vulnerabilities explored.



Vulnerability details and their solutions

Summary Information :

Machine : 192.168.100.40	Selected Profile: testSql

Database: SADATABASE	Selected Profile: testSql

Risk Level	Number of Vulnerabilities	Percentage
Medium	1	5.88%
Low	16	94.12%
Vulnerabilities on SADATABASE	17	100.00%
Vulnerabilities on 192.168.100.40	17	100.00%
Total Vulnerabilities:	17	100.00%

Vulnerability details and their solutions

Machine	**192.168.100.40**
Risk Level	**Medium**
Selected Profile:	testSql

Vulnerability: **Use of SMO and DMO XPs is not disabled.**

Vulnerability's Occurrence::	**1**	**Machine**	192.168.100.40	**Port:**	1,434
Risk Level	Medium	**Product Name**	Sql Server	**Vendor**	Microsoft
Versions	MS SQL Server 2005 and above	**Test Type Name**	Audit		

Vulnerability Information:

Category Name Advanced Checks

Overview: Use of SMO and DMO XPs is not disabled.

Vulnerability References:

References
http://www.springerlink.com/index/h51655j834878664.pdf -
http://msdn.microsoft.com/en-us/library/ms190461.aspx
http://developertechno.blogspot.com/2009/09/disabled-sql-server-2008-database.html

Description

The SMO and DMO XPs are management object extended stored procedures that provide highly-privileged actions that run externally to the DBMS under the security context of the SQL Server service account. If these procedures are available from a database session, an exploit to the SQL Server instance could result in a compromise of the host system and external SQL Server resources including the SQL Server software, audit, log, and data files. Access to these procedures should be disabled unless a clear requirement for their use is indicated and authorized.

Solution

From the query prompt:

exec sp_configure show advanced options,'1'

exec sp_configure SMO and DMO XPs,'0'

reconfigure

The DBA will disable use of external procedures by the database unless mission and/or operationally required it.

Vulnerability Specifications: :

[Name] = SMO and DMO XPs
[Config_Value] = 1

***

***

Vulnerability details and their solutions

Risk Level	Low	Selected Profile:	testSql

Vulnerability: Registry extended proc not removed

Vulnerability's Occurrence::	16	Machine	192.168.100.40	Port:	1,434

Risk Level	Low	Product Name	Sql Server	Vendor	Microsoft
Versions	All versions of Microsoft SQL Server	Test Type Name	Audit		

Vulnerability Information:

Category Name Advanced Checks

Overview: The registry extended stored procedures have not been removed from the database.

Vulnerability References:

References http://www.microsoft.com/TechNet/prodtechnol/sql/proddocs/utilref2/chpt2/75524c02.asp

Description

The registry extended stored procedures allow Microsoft SQL Server to read, write, and enumerate values and keys in the registry. They are used by Enterprise Manager to configure the server.

These procedures should be closely guarded because of the sensitive information stored in the registry. Typical information found in the registry includes password hashes as well as clear text password. The sensitivity of these procedures are exacerbated if Microsoft SQL Server is run under the Windows account Local System. Local System can read and write nearly all values in the registry, even those not accessible by the Administrator.

The list of registry extended stored procedures include:
xp_regaddmultistring
xp_regdeletekey
xp_regdeletevalue
xp_regenumvalues
xp_regenumkeys
xp_regread
xp_regremovemultistring
xp_regwrite
xp_instance_regaddmultistring
xp_instance_regdeletekey
xp_instance_regdeletevalue
xp_instance_regenumkeys
xp_instance_regenumvalues
xp_instance_regread
xp_instance_regremovemultistring
xp_instance_regwrite

If the MSSQLServer service runs under the LocalSystem account, this call will allow a database user to read a password hash out of the registry. The following example demonstrates how this is accomplished:
EXEC xp_regread 'HKEY_LOCAL_MACHINE', 'SECURITY\SAM\Domains\Account', 'F'

Unlike the xp_cmdshell extended stored procedure, which runs under a separate context if executed by a login not in the Sysadmin role, the registry extended stored procedures always execute under the security context of the MSSQLServer service.

By default, the public group has permission to execute xp_regread. All other registry extended stored procedures default to only being executable by the dbo in the master database (typically sysadmins only).

Vulnerability details and their solutions

Solution

You should drop the registry extended stored procedures from the master database. Running the following commands to delete the procedures.

```
sp_dropextendedproc @functname='xp_regaddmultistring'
go
sp_dropextendedproc @functname='xp_regdeletekey'
go
sp_dropextendedproc @functname='xp_regdeletevalue'
go
sp_dropextendedproc @functname='xp_regenumvalues'
go
sp_dropextendedproc @functname='xp_regenumkeys'
go
sp_dropextendedproc @functname='xp_regread'
go
sp_dropextendedproc @functname='xp_regremovemultistring'
go
sp_dropextendedproc @functname='xp_regwrite'
go
sp_dropextendedproc @functname='xp_instance_regaddmultistring'
go
sp_dropextendedproc @functname='xp_instance_regdeletekey'
go
sp_dropextendedproc @functname='xp_instance_regdeletevalue'
go
sp_dropextendedproc @functname='xp_instance_regenumvalues'
go
sp_dropextendedproc @functname='xp_instance_regenumkeys'
go
sp_dropextendedproc @functname='xp_instance_regread'
go
sp_dropextendedproc @functname='xp_instance_regremovemultistring'
go
sp_dropextendedproc @functname='xp_instance_regwrite'
go
```

You should also delete the DLL which houses the stored procedure. This DLL is xpstar.dll. If you do not delete the DLL, a database administrator on the server can simply add the procedure back to the database.

CAUTION: If you drop these procedures or delete the xpstar.dll then some of the applications such as Enterprise Manager will not work properly as they use some of these procedures to configure the MS SQL server. You should drop these procedures and remove the DLL only if you are sure that no production applications use these during normal operations.

Vulnerability Specifications: :

[Object] = xp_instance_regaddmultistring

[Object] = xp_instance_regdeletekey

[Object] = xp_instance_regdeletevalue

[Object] = xp_instance_regenumkeys

[Object] = xp_instance_regenumvalues

[Object] = xp_instance_regread

Vulnerability details and their solutions

[Object] = xp_instance_regremovemultistring

[Object] = xp_instance_regwrite

[Object] = xp_regaddmultistring

[Object] = xp_regdeletekey

[Object] = xp_regdeletevalue

[Object] = xp_regenumkeys

[Object] = xp_regenumvalues

[Object] = xp_regread

[Object] = xp_regremovemultistring

[Object] = xp_regwrite

***

***