secure auditor

Audit Report

Vulnerability categorization by machine

Report Generated Time: 10/13/2011 At 5:58:11PM

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

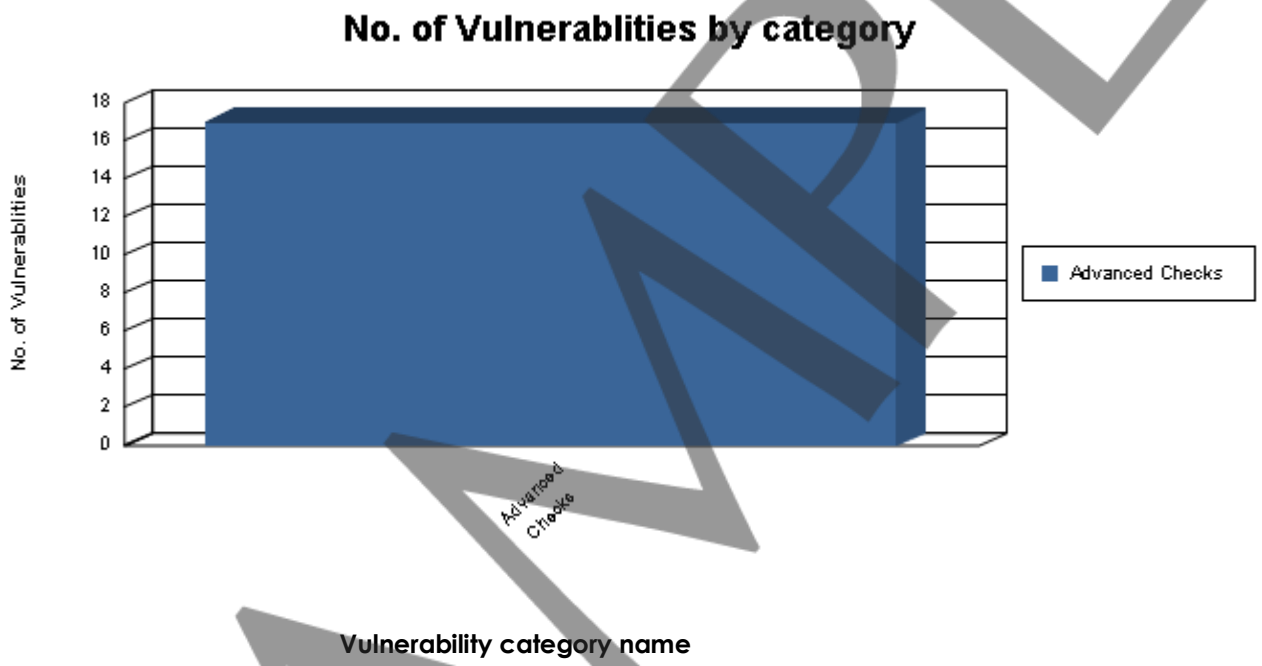
Licensed To : **Support**
Company Name : **Secure Bytes**

SECURE BYTES

Vulnerability categorization by machine

Report generated on 13-Oct-2011 at 5:58:11PM

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 categorization by machine

Category	**Advanced Checks**
Audit Performed :	**SQLServerAudit(Oct 13 2011 5:56PM)**
Selected Profile:	**testSql**
Machine IP	**192.168.100.40**
Machine Port :	**1,434**
Database	**SADATABASE**

Risk Level : Medium

Name Use of SMO and DMO XPs is not disabled.

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.

Risk Level : Low

Name Registry extended proc not removed

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'

Vulnerability categorization by machine

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).

1,954	Vulnerability/ies of type	Advanced Checks

Total Vulnerabilities: 17