SecurityCenter 4

TENABLE NETWORK SECURITY

DISA SQL Server Auditing

March 19, 2012 at 10:27am CDT

Dave Breslin [ddbreslin]

Confidential: The following report contains confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by the recipient company's security policy. All copies and backups of this document should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is grounds for termination.

Table of Contents

Configuration Audit Summary

Compliance Checks. Info = Pass, Medium = Couldn't Execute, High = Fail

IP Address	NetBIOS Name	Info	Med.	High
10.200.0.2	ITSDEPT\SQLDEV	118	1	2
10.101.0.2	ITSDEPT\SQLQA	116	1	4
10.100.0.2	ITSDEPT\SQLPROD	114	2	5

Patch Audit Summary

Microsoft Bulletins. CVSS Ranges; Low = 0.1 - 3.9, Medium = 4.0 - 6.9, High = 7.0 - 9.9, Critical = 10

IP Address	NetBIOS Name	Info	Low	Med.	High	Crit.
10.200.0.2	ITSDEPT\SQLDEV	0	0	0	2	0
10.101.0.2	ITSDEPT\SQLQA	0	0	0	2	0
10.100.0.2	ITSDEPT\SQLPROD	0	0	0	2	0

Configuration Audit Details - Fails and Couldn't Execute

10.100.0.2

NetBIOS Name: ITSDEPT\SQLPROD	
Last Scan: Feb 16, 2012 @ 9:18PM	

Configuration Audit Details. Medium = Couldn't Execute, High = Fail

Severity	Plugin Name
High	3.165 DM1715: Unauthorized object permission grants (master)
Medium	3.155 DM1709: Guest user (distribution)
Medium	3.154 DM0630: Application object owner account disabling (distribution)
High	3.131 DM0500: SYSADMIN fixed server role membership
High	3.24 DM6161: xp_cmdshell option
High	3.17 DM6010: Rename sa account
High	3.9 DG0125: DBMS account password expiration

10.101.0.2

NetBIOS Name: ITSDEPT\SQLQA	
Last Scan: Feb 16, 2012 @ 9:18PM	

Configuration Audit Details. Medium = Couldn't Execute, High = Fail

Severity	Plugin Name
Medium	3.147 DM6123: clr enabled option
High	3.139 DM2142: Remote access option
High	3.138 DM2133: Replication use and security
High	3.136 DM2095: OLE Automation Procedures (option)
High	3.134 DM1761: Scan for startup procs option (value_in_use)

10.200.0.2

NetBIOS Name: ITSDEPT\SQLDEV	
Last Scan: Feb 16, 2012 @ 9:18PM	

Configuration Audit Details. Medium = Couldn't Execute, High = Fail

Severity	Plugin Name
Medium	3.129 DG0120: Application user access to external objects (distribution)
High	3.27 DM6199: SMO and DMO XPs option
High	3.17 DM6010: Rename sa account

Patch Audit Details - All Microsoft Bulletins

10.100.0.2

NetBIOS Name: ITSDEPT\SQLPROD
Last Scan: Feb 16, 2012 @ 9:18PM

Patch Audit Details. CVSS Ranges; Low = 0.1 - 3.9, Medium = 4.0 - 6.9, High = 7.0 - 9.9, Critical = 10

Plugin	Severity	Plugin Name
57942	High	MS12-008: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)
57943	High	MS12-009: Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640)

10.101.0.2

NetBIOS Name: ITSDEPT\SQLQA	
Last Scan: Feb 16, 2012 @ 9:18PM	

Patch Audit Details. CVSS Ranges; Low = 0.1 - 3.9, Medium = 4.0 - 6.9, High = 7.0 - 9.9, Critical = 10

Plugin	Severity	Plugin Name
57942	High	MS12-008: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)
57943	High	MS12-009: Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640)

10.200.0.2

NetBIOS Name: ITSDEPT\SQLDEV	
Last Scan: Feb 16, 2012 @ 9:18PM	

Patch Audit Details. CVSS Ranges; Low = 0.1 - 3.9, Medium = 4.0 - 6.9, High = 7.0 - 9.9, Critical = 10

Plugin	Severity	Plugin Name
57942	High	MS12-008: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)
57943	High	MS12-009: Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640)