安全配置基线检测分析报告

主机报告

北京奇安信集团

2019 年 11 月 19 日

版权说明

保密申明

目录

一. 主机概述

主机风险	非常危险 11.1（分）		
IP 地址	10.194.67.165		
扫描时间	2019-11-19 12:57:24.776325+08:00		
配置检查模板	SQL Server 基线配置规范		
平均符合度	25.0%		
检查项总数	12	合规检查项总数	3
不合规检查项总数	9	高危不合规个数	4
中危不合规个数	2	低危不合规个数	3

二. 安全配置基线检测结果

2.1 总体评价

本次对 10.194.67.165 主机进行 SQL Server 基线配置规范检测，其中发现主机存在安全风险。建议业务管理负责人通过**《安全配置基线检测分析报告-主机报告》**第一时间完成安全问题确认及配置加固，并持续完善和优化信息安全管控措施。建议常态化监督安全保障措施的执行落地，确保各类业务尤其是互联网业务的安全运营和可管、可控。

2.2 检测列表

序号	检查项名称	检查类别	风险级别	是否合规
1	检查是否按照责任、权限创建、使用用户账号	账号口令	中危	不合规
2	检查是否已删除高危用户账号	账号口令	高危	合规
3	检查用户的属性是否安全	其它安全	低危	不合规
4	检查是否强制实施密码策略(密码复杂度)	账号口令	高危	不合规
5	检查是否强制密码过期	账号口令	低危	不合规
6	检查通讯协议是否加密	协议安全	高危	不合规
7	检查身份验证设置是否安全	访问控制	高危	不合规
8	检查审核级别设置是否安全	其它安全	低危	不合规
9	检查是否已停用高危存储过程	其它安全	中危	不合规
10	检查是否升级系统版本及补丁包版本	其它安全	高危	不合规
11	检查是否已配置最大并发连接数	远程管理	高危	合规
12	检查是否已更改服务器监听端口号	系统服务	低危	合规

三. 配置不合规问题详述

3.1 检查是否按照责任、权限创建、使用用户账号

3.1.1 检查 SQL Server 用户账号个数

检测名称	检查 SQL Server 用户账号个数
风险级别	中危
修复建议	打开 SQL Server Management Studio（在 SQL Server 2000 下打开企业管理器），登入相应的数据库实例，依次展开“安全性”、“登录名”（在 SQL Server 2000 下为“登录”）节点，创建多个账户，按照实际情况赋予账户相应的角色

检测规则	大于等于
期望值	2
真实值	

3.2 检查用户的属性是否安全

3.2.1 检查密码为空的 SQL Server 用户的个数

检测名称	检查密码为空的 SQL Server 用户的个数
风险级别	低危
修复建议	打开 SQL Server Management Studio（在 SQL Server 2000 下打开企业管理器），登入相应的数据库实例，依次展开“安全性”、“登录名”（在 SQL Server 2000 下为“登录”）节点，为所有 SQL Server 用户（使用 SQL Server 身份验证的用户）设置密码。
检测规则	相等
期望值	0
真实值	

3.3 检查是否强制实施密码策略(密码复杂度)

3.3.1 检查未设置“强制实施密码策略”的 SQL Server 用户的个数

检测名称	检查未设置“强制实施密码策略”的 SQL Server 用户的个数
风险级别	高危
修复建议	在 SQL Server 2005 及以上版本的 SQL Server 中，打开 SQL Server Management Studio，连接相应的数据库实例，依次展开“安全性”、“登录名”节点，打开相应的帐户的属性，选择“常规”选项卡，勾选“强制实施密码策略”；在 SQL Server 2000 中，请手动检查。
检测规则	相等
期望值	0
真实值	

3.4 检查是否强制密码过期

3.4.1 检查未设置“强制密码过期”的 SQL Server 用户的个数

检测名称	检查未设置“强制密码过期”的 SQL Server 用户的个数
风险级别	低危
修复建议	在 SQL Server 2005 及以上版本的 SQL Server 中，打开 SQL Server Management Studio，登入相应的数据库实例，依次展开“安全性”、“登录名”节点，打开相应的帐户的属性，选择“常规”选项卡，勾选“强制密码过期”；在 SQL Server 2000 中，请手动检查。
检测规则	相等
期望值	0
真实值	

3.5 检查通讯协议是否加密

3.5.1 检查通讯协议是否加密

检测名称	检查通讯协议是否加密
风险级别	高危
修复建议	在 SQL Server 2000 中打开 SQL Server 服务器网络实用工具，选择相应的数据库实例，点选“强制协议加密”；在 SQL Server 2005 及以上版本的 SQL Server 中，打开 SQL Server Configuration Manager（配置管理器），展开“SQL Server 网络配置”节点，打开相应的数据库实例的属性对话框，将“ForceEncryption”（强行加密）设置为“是”。启用“加密”功能需要安装有效证书，否则，SQL Server 2000 将无法启动，SQL Server 2005 及以上版本的 SQL Server 将使用不安全的自签名证书。 设置完成后需要重启数据库才能生效。
检测规则	字符串相等
期望值	TRUE
真实值	

3.6 检查身份验证设置是否安全

3.6.1 检查 “服务器身份验证”模式

检测名称	检查 “服务器身份验证”模式
风险级别	高危
修复建议	打开 SQL Server Management Studio（在 SQL Server 2000 下打开企业管理器），连接相应的数据库实例，在数据库名称上点击右键，打开其属性对话框，选择“安全性”选项卡，将“服务器身份验证”（在 SQL Server 2000 下为“身份验证”）更改为“SQL Server 和 Windows 身份验证模式”（在 SQL Server 2000 下为“SQL Server 和 Windows”），并重启数据库使之生效。
检测规则	字符串相等
期望值	SQLServer+Windows
真实值	

3.7 检查审核级别设置是否安全

3.7.1 检查 “登录审核”级别

检测名称	检查 “登录审核”级别
风险级别	低危
修复建议	打开 SQL Server Management Studio（在 SQL Server 2000 下打开企业管理器），连接相应的数据库实例，在数据库名称上点击右键，打开其属性对话框，选择“安全性”选项卡，将“登录审核”（在 SQL Server 2000 下为“审核级别”）更改为“失败和成功的登录”（在 SQL Server 2000 下为“全部”），并重启数据库使之生效。
检测规则	字符串相等
期望值	Success+Fail
真实值	

3.8 检查是否已停用高危存储过程

3.8.1 检查高危存储过程

检测名称	检查高危存储过程
风险级别	中危
修复建议	1. 高 危 sp_OACreate,sp_OADestroy,sp_OAGetErrorInfo,sp_OAGetProperty,sp_OAMethod,sp_OASetProperty,sp _enumerrorlogs,xp_enumgroups,xp_enumqueuedtasks,xp_eventlog,xp_findnextmsg,xp_fixeddrives,xp_g p_schedulersignal,xp_sendmail,xp_servicecontrol,xp_snmp_getstate,xp_snmp_raisetrap,xp_sprintf,xp_sq 2. 在 SQL Server 2000 中打开企业管理器，连接相应的数据库实例，依次展开数据库、master、扩展存储 上版本的 SQL Server 中打开 SQL Server Management Studio，连接相应的数据库实例，依次展开数据库
检测规则	字符串相等
期望值	AllSafe
真实值	

3.9 检查是否升级系统版本及补丁包版本

3.9.1 检查 SQL Server 系统版本及补丁包版本

检测名称	检查 SQL Server 系统版本及补丁包版本
风险级别	高危
修复建议	请到微软官方网站下载对应 SQL Server 最新补丁包并安装。SQL Server 2000 最新补丁包是 SP4，SQL Server 2005 是 SP4，SQL Server 2008 是 SP3，SQL Server 2008 R2 是 SP2，SQL Server 2012 是 SP1。
检测规则	正则表达式匹配
期望值	/(2000SP4)|(2005SP4)|(2008SP3)|(2008R2SP2)|(2012SP1)/
真实值	

四. 附录信息

4.1 Windows 主机名

主机名
database-database

4.2 SQL Server 实例信息

实例名
ECHO 处于打开状态。

4.3 Windows 用户信息

用户名	用户描述	用户是否被锁定	密码是否可更改	密码是否到期	是否需要密码	是否启用

DATABASE-DATABA\Administrator	管理计算机(域)的内置帐户	FALSE	TRUE	TRUE	TRUE	OK
DATABASE-DATABA\cloudbase-init		FALSE	FALSE	FALSE	TRUE	OK
DATABASE-DATABA\Guest	供来宾访问计算机或访问域的内置帐户	FALSE	FALSE	FALSE	FALSE	Degraded

4.4 Windows 系统信息

系统	版本

Microsoft Windows Server 2012 R2 Datacenter	6.3.9600

五. 参考标准

5.1 配置检查项风险等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <= 检查项风险值 <= 10	不当的配置导致攻击者可以通过其他方式获得管理员权限、或者只有管理员权限才能加固的配置。
中	4 <= 检查项风险值 < 7	不当的配置导致攻击者可以对主机进行破坏或者收集主机的信息、或者遭受攻击后，重要事件没有记录。
低	0 <= 检查项风险值 < 4	不当地配置对主机安全不会造成太大的影响。

5.2 资产风险等级评定标准

资产风险等级	资产风险值区域
非常危险	7 <= 资产风险值 <= 10
比较危险	5 <= 资产风险值 < 7
比较安全	2 <= 资产风险值 < 5
非常安全	0 <= 资产风险值 < 2

说明：

1、将资产的风险等级按照分数的高低排序，依据配置检查项的分数将配置威胁划分为高、中、低三个类别。

2、按照风险评估模型计算得到风险值。

3、注：高、中和低配置威胁的定义参见《配置检查项风险等级评定标准》。

4、非常危险的资产定义为高风险；比较危险的资产定义为中风险；比较安全和非常安全的资产定义为低风险。

5.3 等级保护等级划分标准

《信息安全等级保护管理办法》规定，国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

信息系统的安全保护等级分为以下五级，一至五级等级逐级增高：

受侵害客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序和公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

按照《信息系统等级保护基本要求》定义的 S\A\G 要求项，其中 S 表示业务信息安全相关要求，A 表示系统服务保证相关要求，G 表示通用安全保护要求。后面的数字代表等级，S3 的意思也就是信息安全类 3 级要求，以此类推。

其中，按照 S\A\G 要求项组合可实现等级保护的定级：

安全等级	信息系统保护要求组合
第一级	S1A1G1
第二级	S1A2G2，S2A2G2，S2A1G2
第三级	S1A3G3，S2A3G3，S3A3G3，S3A2G3，S3A1G3
第四级	S1A4G4，S2A4G4，S3A4G4，S4A4G4，S4A3G4，S4A2G4，S4A1G4

5.4 安全建议

随着越来越多的网络访问通过系统漏洞进行操作，系统漏洞已成为互联网安全的一个热点，基于系统漏洞的攻击广为流行，CGI 攻击检测、网络设备和防火墙、本地安全检查等问题严重威胁着系统管理者和系统用户的安全，我们有必要采取措施消除这些风险。

建议对存在漏洞的资产参考附件中提出的解决方案进行漏洞修补、安全增强。

- 建议对存在不合规检查项的主机参考对应的检查点详情中提出的调整方案和标准值进行修正。
- 请专业的安全研究人员或安全公司对系统架构做全面的安全审计，修补所有发现的安全漏洞。
- 对系统的开发人员进行安全编码方面的培训，在开发过程避免漏洞的引入能起到事半功倍的效果。
- 采用专业的系统安全产品，可以在不修改系统本身的情况下

对大多数的基于漏洞攻击起到有效的阻断作用，提供了强大的扫描产品，可以满足用户在这方面的需求。

- 建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞，特别是影响到漏洞站点所使用的系统和软件的漏洞，应该在事前设计好应对规划，一旦发现系统受漏洞影响及时采取措施。