数据库安全保护不能忽略最简单的漏洞

企业必须对数据库进行评估来确定某些功能是否真的必要，以及禁用那些不需要的功能来减少攻击面。此外，企业必须对默认设置或者较弱的登录凭证时刻保持警惕，必须部署完善的特权和身份验证措施，最重要的是，企业需要定期修复补丁。

在所发现的漏洞中，有将近一半的漏洞或直接或间接地与数据库环境内不适当的补丁修复管理有关。这是很恐怖的概念：在前三个月补丁修复周期内，只有 38%的管理员修复企业的 Oracle 数据库，并且只有三分之一的管理员花费一年或者更长时间进行修复。

1. 默认、空白和强度弱的用户名或者密码

在一个企业中，跟踪数百或者甚至数千个数据库可能是很艰巨的任务，但是删除默认、空白以及强度弱的登录凭证将是完善数据库安全非常重要的第一个步骤。攻击者们总是将注意力放在这些默认帐户上，必要的时候就能派上用场。

2. SQL 注入攻击

SQL 注入攻击是黑客对数据库进行攻击的常用手段之一。随着 B/S 模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多，但是由于程序员的水平及经验也参差不齐，相当大一部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据，这就是所谓的 SQL Injection，即 SQL 注入。

如果企业数据库平台无法对输入内容进行审查，攻击者将能够执行 SQL 注入攻击，就像在 web 攻击中所做的那样，SQL 注入攻击最终将允许攻击者提升权限，并且获取对更广泛功能的访问权限。很多供应商发布了修复程序来避免这些问题，但是如果 DBMS 仍然未打补丁，这些修复程序也帮不了企业管理者。

3.广泛的用户和组特权

企业必须确保没有将特权给那些不必要的用户。安全专家建议，只有将用户设置为组或者角色的一部分，然后通过这些角色来管理权限，这样将比向用户分配直接权利要更加易于管理。

4.启用不必要的数据库功能

每个数据库安装都会附带各种类型各种大小的功能，并且大部分都不会被企业所使用。数据库安全意味着减少攻击面，企业需要审查这些数据库功能，找出不必要或者不使用的功能，然后禁用或者卸载它们。这不仅能够降低通过这些载体发动的零日攻击的风险，而且能够简化补丁修复管理，因为这些不必要的功能也需要进行补丁修复。

5.糟糕的配置管理

同样地，数据库有很多不同的配置可供选择，正确合适的配置将能够帮助数据库管理员提高数据库性能和加强数据库功能。企业需要找出不安全的配置(默认情况下为启用状态或者为了方便数据库管理员或者应用程序开发人员而开启的)，然后重新进行配置。

6.缓冲区溢出

另一个攻击者喜欢的漏洞就是缓冲区溢出漏洞，这个漏洞是这样被利用的，即大量输入比应用程序预期更多的字符，例如向请求 SSN 的输入框增加 100 个

字符。数据库供应商都在积极努力地修复这个漏洞，以避免发生这样的攻击，这也是为什么补丁修复如此重要的另一个原因。

7. 特权升级

同样的，数据库常常出现这样的漏洞，允许攻击者对鲜为人知或者低权限帐号进行权限升级，然后获取管理员权限。例如，攻击者可能误用 sysdba 下运行的一个函数。由于这些漏洞还没有被发现，管理员需要即使更新和修复补丁来防止这种漏洞被利用。

8.拒绝服务攻击

拒绝服务攻击即攻击者想办法让目标机器停止提供服务，是黑客常用的攻击手段之。其实对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。拒绝服务攻击问题也一直得不到合理的解决，究其原因是因为这是由于网络协议本身的安全缺陷造成的，从而拒绝服务攻击也成为了攻击者的终极手法。攻击者进行拒绝服务攻击，实际上让服务器实现两种效果：一是迫使服务器的缓冲区满，不接收新的请求;二是使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接

SQL Slammer 是关于攻击者如何利用 DBMS 漏洞来通过大量流量攻破数据库服务器的非常具有启发意义的例子，而更具启发性的是，当在 2003 年 Slammer 沦陷后，已经出现了解决这个漏洞的补丁修复程序，然而，即使在七年后的今天，SQL Slammer 仍然在作恶多端，攻击那些未修复的服务器。

9.未修复数据库与未加密重要数据(静态或者动态状态)

这一点可能与上述漏洞有些重复，但是这值得再次重复。很多数据库管理员并没有及时修复补丁，因为他们害怕补丁修复程序将会破坏他们的数据库。但是现在，被攻击的风险比安装可能会破坏数据库的补丁要高得多，而这在五年前可能并不是这样，但是供应商现在已经更加严格的进行测试