3.9 安全加固(重点)

详见文档

WSUS(一个一个打补单)、批处理的方式打补丁。

1.1.1.2. 操作系统加固

编号	Windows-02001
名称	补丁安装
当前状态：	OS Hot Fix Installed Q147222 2009-2-18
实施方案	使用 Windows update 安装最新补丁
回退方案	【并不是所有内容都能回退，要和相关人员（运维人员）讨论】
实施目的	可以使系统版本为最新版本
实施风险	安装补丁可能导致主机启动失败，或其他未知情况发生

是否加固	□执行加固 □不执行加固 原因：
执行人员	□AAA □第三方

编号	Windows-05003
名称	限制特定系统文件的权限
当前状态：	未对 C、D、E、windows\system、windows\system32 等敏感执行文件设置合适的权限
实施方案	选择 windows\system 等相应的文件夹，右键选择“属性”>“安全”，将 everyone 组和 users 组的权限设置为只读，而 administrator 组拥有完全控制权
实施目的	重要目录不能对 everyone 开放，这样会带来很大的安全问题。
实施风险	对于某一具体系统要具体问题具体分析，尤其要注意对于应用系统的影响。
是否加固	□执行加固 □不执行加固 原因：
执行人员	□AAA □第三方

编号	Windows-07001
名称	保护注册表，防止匿名访问
当前状态：	Everyone 存在，并带有一定权限。
实施方案	运行|regedit| 转到 HKLM\SYSTEM\CurrentControlSet\Control\ SecurePipeServers\winreg 删除 everyone 的所有权限
实施目的	保护注册表
实施风险	无风险
是否加固	□执行加固 □不执行加固 原因：
执行人员	□AAA □第三方

编号	Windows-07002
名称	对匿名连接的额外限制
当前状态：	不允许 SAM 帐户和共享的匿名枚举 已禁用
实施方案	方法一： Key:HKLM\SYSTEM\CurrentControlSet\Control\Lsa “restrictanonymous”的值为 0 修改相应的安全策略文件将该值修改为“1” 方法二： 开始|管理工具|本地安全策略|本地策略|安全选项| 双击 网络访问：不允许 SAM 帐户和共享的匿名枚举 将其改为已启用
实施目的	可以禁止匿名用户列举主机上所有用户、组、共享资源
实施风险	无
是否加固	□执行加固 □不执行加固 原因：
执行人员	□AAA □第三方

1.1.1.3.漏洞扫描加固

无。

补丁(90-95%)

弱口令(弱账户)

配置漏洞