常见安全漏洞加固

2019护网专题培训

NSFOCUS

CONTENTS 目 录

01

常见漏洞分类简述

1. 常见系统漏洞分类
2. 常见WEB漏洞分类

NSFOCUS

1.1

常见系统漏洞分类

CNNVD漏洞分类

漏洞类型描述

配置错误

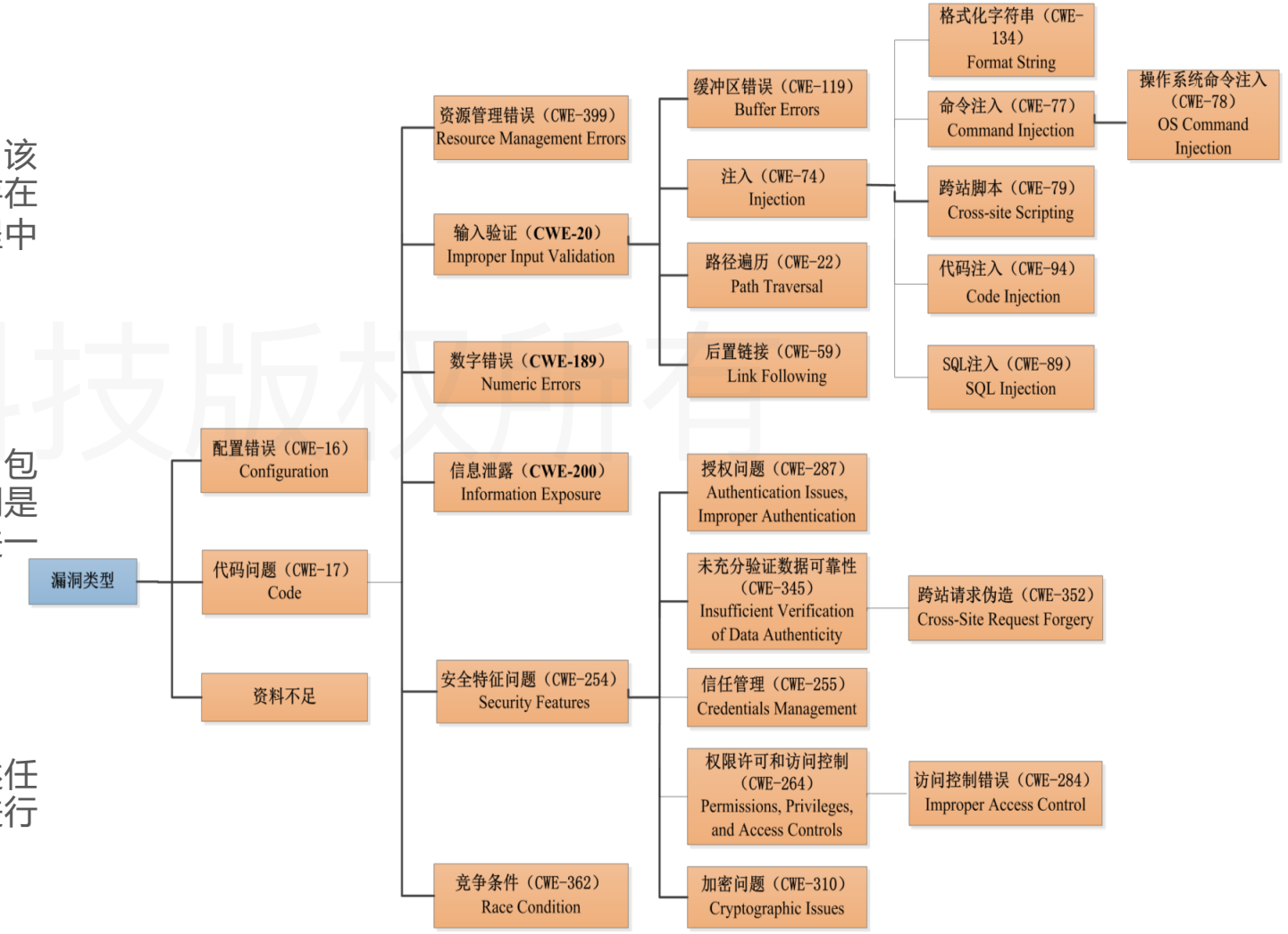
此类漏洞指软件配置过程中产生的漏洞。该类漏洞并非软件开发过程中造成的，不存在于软件的代码之中，是由于软件使用过程中的不合理配置造成的内容添加内容

代码问题

此类漏洞指代码开发过程中产生的漏洞，包括软件的规范说明、设计和实现。该漏洞是一个高级别漏洞，如果有足够的信息可进一步分为更低级别的漏洞

资料不足

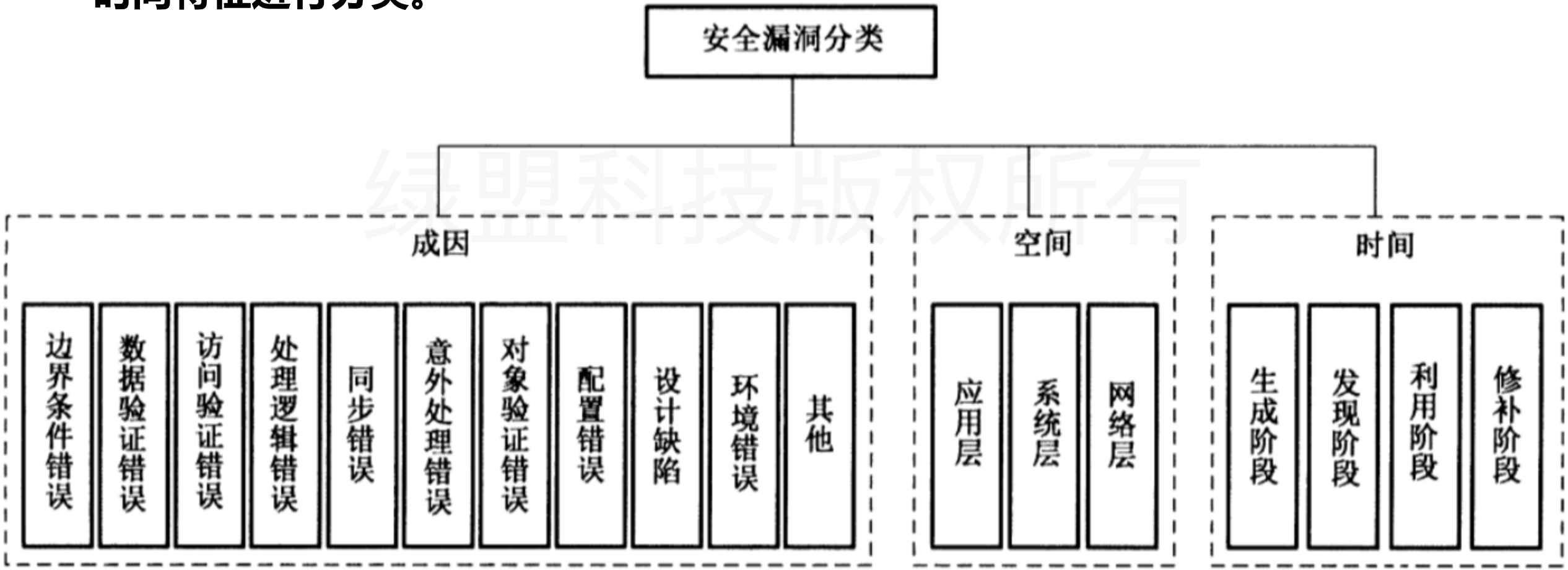
根据目前信息暂时无法将该漏洞归入上述任何类型，或者没有足够充分的信息对其进行分类，漏洞细节未指明内容



NSFOCUS

GB/T 33561-2017漏洞分类

依据国标信息安全技术—安全漏洞分类标准，按照形成原因、所处空间和时间特征进行分类。



其他漏洞分类

基于利用位置的分类

- 本地漏洞
- 远程漏洞

基于威胁类型的分类

- 获取控制
- 获取信息
- 拒绝服务

基于技术类型的分类

- 内存破坏类
- 逻辑错误类
- 输入验证类
- 设计错误类
- 配置错误类

02

常见操作系统漏洞加固

1. MS07-010漏洞加固方案
2. SSH漏洞加固方案

NSFOCUS

2.1

MS07-010漏洞加固方案

远程代码执行漏洞(MS17-010)加固

启动会

① 对安全加固活动进行宣讲

② 落实服务所需的人员、设备、资料等资源

实施加固计划

① 明确的项目组织及职责；

② 明确的项目实施阶段各项工作任务的内容及要求，以及工程和环节的逻辑顺序；

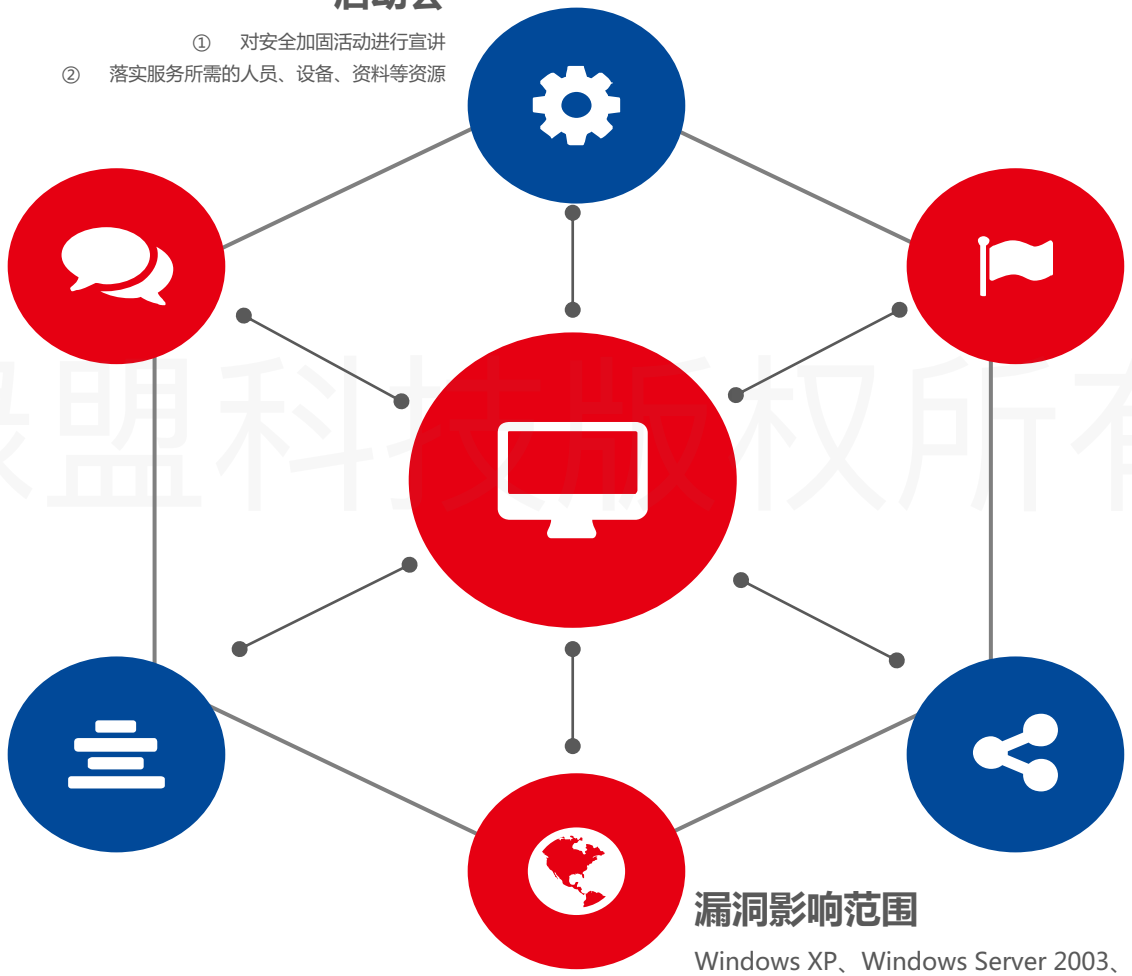
③ 编制分时间阶段的实施进度表，使所有工作任务正确地定位并考虑完成每项任务有充分的时间；

④ 确定每项任务需要的资源，以保证项目实施时期获得足够的支持；

⑤ 将所有实施数据计入文件，以便使实施计划能做出及时修订。

实施加固清单

明确项目范围内的系统资产存在漏洞的IP地址



漏洞描述

① SMB协议是一个通过网络在共享文件、打印设备、命名管道、邮槽之间操作数据的协议。利用该协议，客户端就可以去访问服务器上的共享文件和目录（增删改查）、打印队列和进程间通信服务等，还可以实现客户端和服务器之间的远程过程子协议的认证传输。

② Windows的SMB服务处理 SMBv1 接收的特殊设计的数据包，发生缓冲区溢出，导致攻击者在目标系统上可以执行任意代码。

漏洞威胁

能远程主动发起对漏洞主机135\137\138\139\445端口的扫描，并且能直接获得漏洞主机的系统权限，属于最高严重级别的漏洞。

漏洞影响范围

Windows XP、Windows Server 2003、Windows Vista、Windows Server 2008、Windows 7、Windows Server 2008 R2、Windows 8.1、Windows Server 2012、Windows 10、Windows Server 2012 R2、Windows Server 2016

NSFOCUS

远程代码执行漏洞(MS17-010)加固

- **加固方案：1. 安装最新补丁，下载漏洞影响范围所有的补丁，并做好区分标识。**

  注意事项：安装补丁前查看当前windows版本(“我的电脑”右键选择“属性”)

readme.ini - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
[winxpsp3_x86]
kb4012598 = .\hotfix\windowsxp-kb4012598-x86-custom-chs_dca9b5adddad778cfd4b7349ff54b5167
[winxpsp2_x64]
kb4012598 = .\hotfix\windowsserver2003-kb4012598-x64-custom-chs_68a2895db36e911af59c2ee133

[win2003sp2_x86]
kb4012598 = .\hotfix\windowsserver2003-kb4012598-x86-custom-chs_b45d2d8c83583053d37b20edf5
[win2003sp2_x64]
kb4012598 = .\hotfix\windowsserver2003-kb4012598-x64-custom-chs_68a2895db36e911af59c2ee133

[win7sp1_x86]
kb4012212 = .\hotfix\windows6.1-kb4012212-x86_6bb04d3971bb58ae4bac44219e7169812914df3f.msu
kb4012215 = .\hotfix\windows6.1-kb4012215-x86_e5918381cef63f171a74418f12143dabe5561a66.msu

[win7sp1_x64]
kb4012212 = .\hotfix\windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu
kb4012215 = .\hotfix\windows6.1-kb4012215-x64_a777b8c251dcd8378ecdafa81aefbe7f9009c72b.msu

[vista_x86]
kb4012598 = .\hotfix\windows6.0-kb4012598-x86_13e9b3d77ba5599764c296075a796c16a85c745c.msu

[vista_x64]
kb4012598 = .\hotfix\windows6.0-kb4012598-x64_6a186ba2b2b98b2144b50f88baf33a5fa53b5d76.msu

[win2008sp2_x86]
kb4012598 = .\hotfix\windows6.0-kb4012598-x86_13e9b3d77ba5599764c296075a796c16a85c745c.msu

[win2008sp2_x64]
kb4012598 = .\hotfix\windows6.0-kb4012598-x64_6a186ba2b2b98b2144b50f88baf33a5fa53b5d76.msu
```

readme.ini - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
[win2008r2sp1_x86]
kb4012212 = .\hotfix\windows6.1-kb4012212-x86_6bb04d3971bb58ae4bac44219e7169812914df3f.msu
kb4012215 = .\hotfix\windows6.1-kb4012215-x86_e5918381cef63f171a74418f12143dabe5561a66.msu

[win2008r2sp1_x64]
kb4012212 = .\hotfix\windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu
kb4012215 = .\hotfix\windows6.1-kb4012215-x64_a777b8c251dcd8378ecdafa81aefbe7f9009c72b.msu

[win8.1_x86]
kb4012213 = .\hotfix\windows8.1-kb4012213-x86_e118939b397bc983971c88d9c9ecc8cbec471b05.msu
kb4012216 = .\hotfix\windows8.1-kb4012216-x86_d4facfdaf4b1791efbc3612fe299e41515569443.msu

[win8.1_x64]
kb4012213 = .\hotfix\windows8.1-kb4012213-x64_5b24b9ca5a123a844ed793e0f2be974148520349.msu
kb4012216 = .\hotfix\windows8.1-kb4012216-x64_cd5e0a62e602176f00787785487796e2d47cfa15b.msu

[win2012_x64]
kb4012214 = .\hotfix\windows8-rt-kb4012214-x64_b14951d29cb4fd880948f5204d54721e64c9942b.msu
kb4012217 = .\hotfix\windows8-rt-kb4012217-x64_96635071602f71b4fb2f1a202e99a5e21870bc93.msu

[win2012r2_x64]
kb4012213 = .\hotfix\windows8.1-kb4012213-x86_e118939b397bc983971c88d9c9ecc8cbec471b05.msu
kb4012216 = .\hotfix\windows8.1-kb4012216-x86_d4facfdaf4b1791efbc3612fe299e41515569443.msu

[win8_x86]
kb4012598 = .\hotfix\windows8-rt-kb4012598-x86_a0f1c953a24dd042acc540c59b339f55fb18f594.msu
[win8_x64]
kb4012598 = .\hotfix\windows8-rt-kb4012598-x64_f05841d2e94197c2dca4457f1b895e8f632b7f8e.msu
```

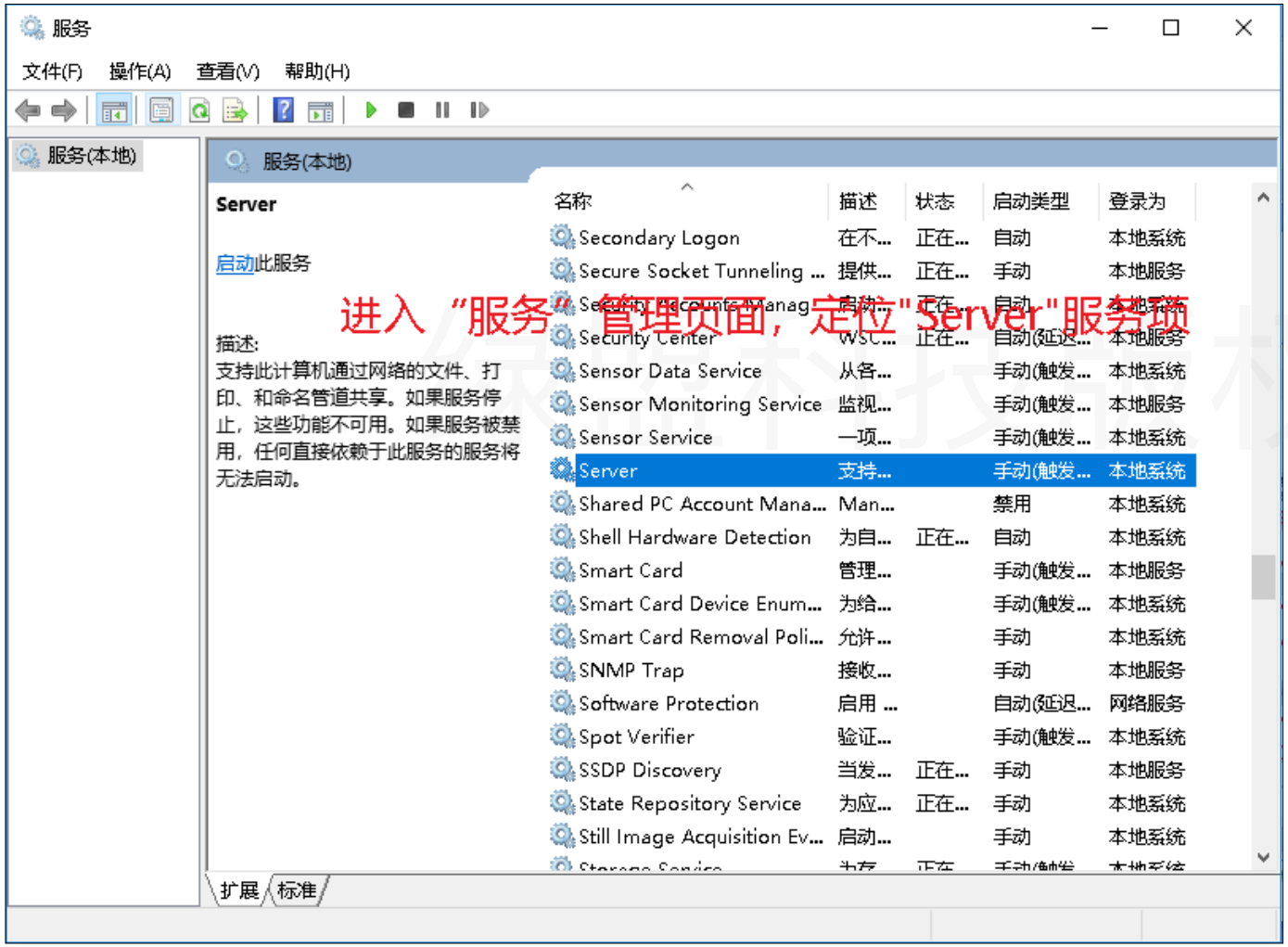
远程代码执行漏洞(MS17-010)加固

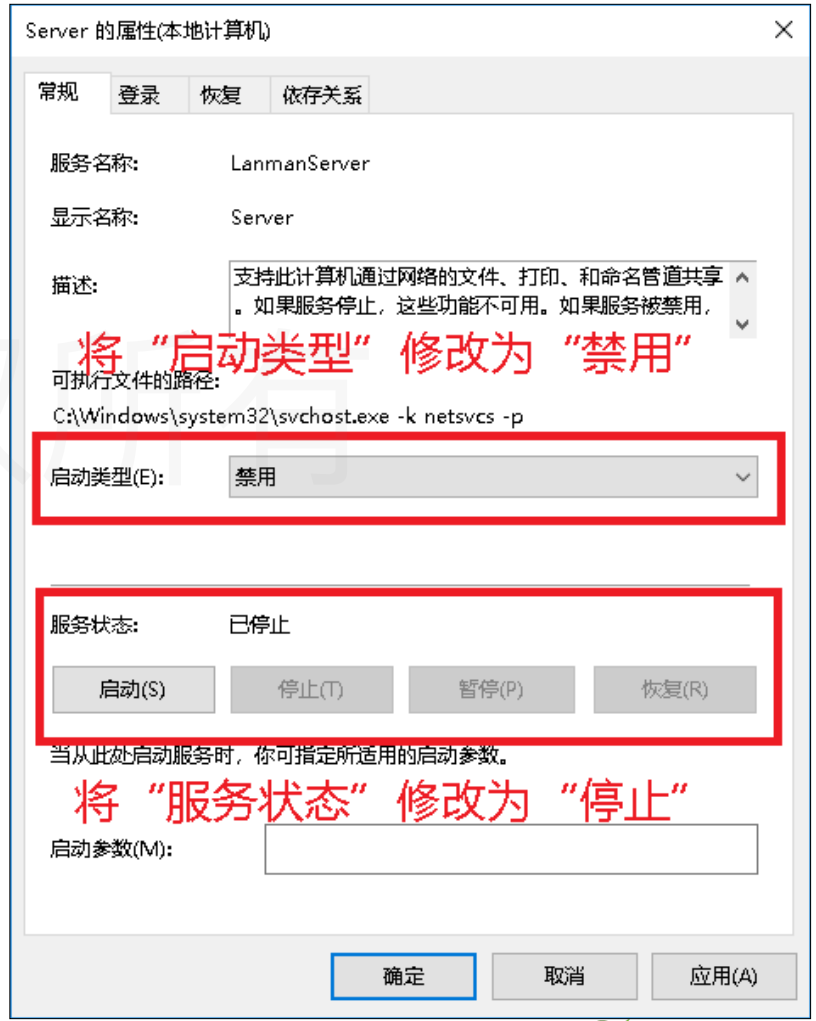
加固方案：2. 禁用服务器服务

- 单击“开始”，然后单击“控制面板”（或指向“设置”，然后单击“控制面板”）
- 双击“管理工具”
- 双击“服务”
- 双击“Server”
- 在“启动类型”列表中，单击“禁用”
- 单击“停止”，然后单击“确定”

远程代码执行漏洞(MS17-010)加固

通过禁用“Server”服务，关闭受影响的445端口。





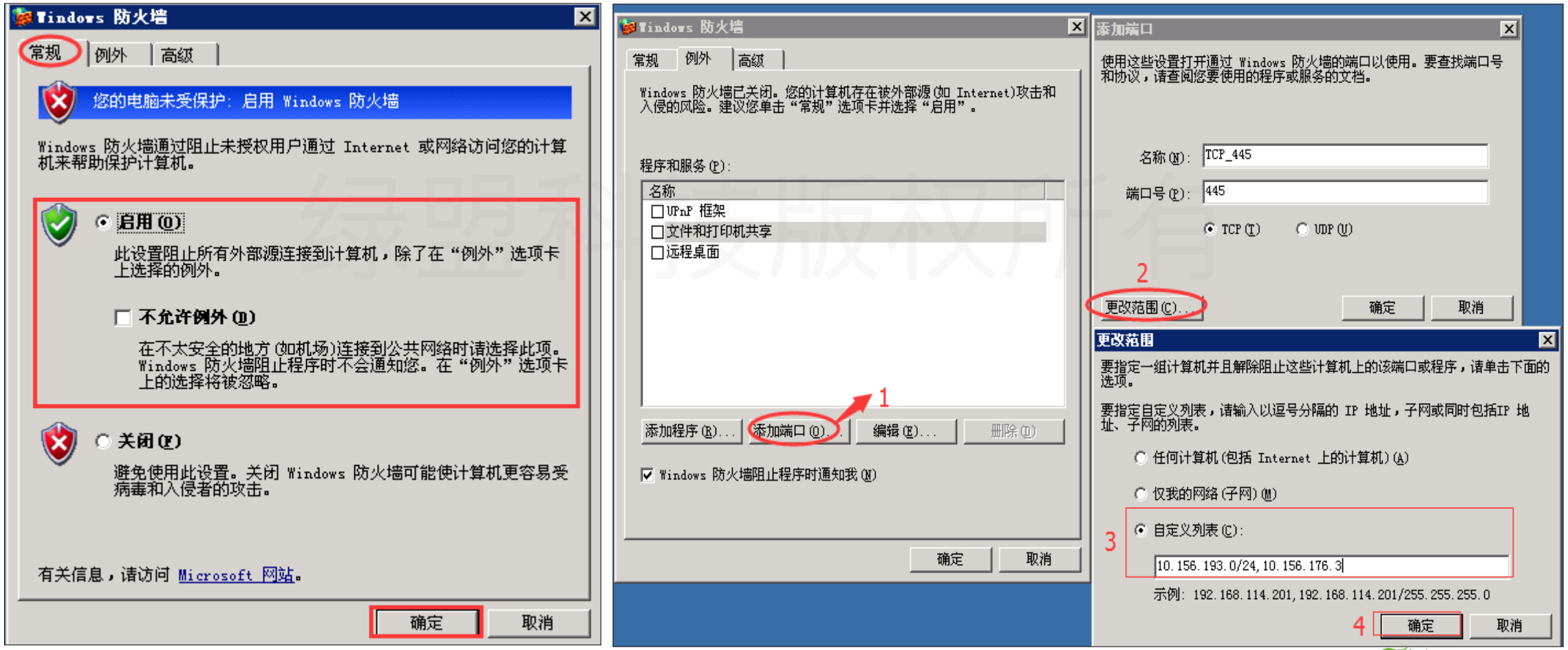
NSFOCUS

远程代码执行漏洞(MS17-010)加固

- **加固方案：3. 在防火墙处阻止 TCP 端口 135、137、138、139 和 445**
  - **Windows XP 系统，使用网络安装向导启用 Windows 防火墙**
    - 单击“开始”，然后单击“控制面板”。
    - 双击“网络连接”，然后单击“更改 Window 防火墙设置”。
    - 在“常规”选项卡上，确保选择了“启用（推荐）”。 这将启用 Windows 防火墙。
    - 启用 Windows 防火墙之后，请选择“不允许例外”以阻止所有传入的通信。
  - **Windows Server 2003 系统，使用网络安装向导启用 Windows 防火墙**
    - 单击“开始”，然后单击“控制面板”。
    - 在默认的“分类视图”中，单击“网络和 Internet 连接”，然后单击“网络连接”。
    - 右键单击要启用“Internet 连接防火墙”的连接，然后单击“属性”。
    - 单击“高级”选项卡。
    - 选中“通过限制或阻止来自 Internet 的对此计算机的访问来保护我的计算机或网络”复选框，然后单击“确定”。

远程代码执行漏洞(MS17-010)加固

通过开启防火墙功能，阻止访问受影响的445端口。同时，可以设置白名单，允许受信的主机访问。



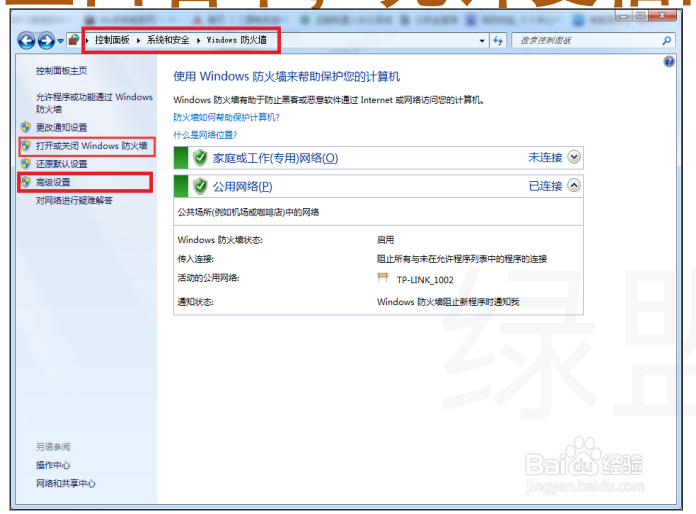
远程代码执行漏洞(MS17-010)加固

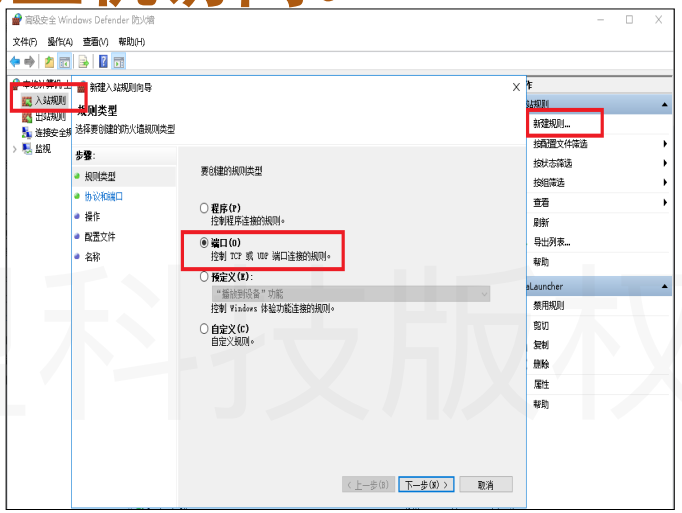
Windows Vista以上系统，使用网络安装向导启用 Windows 防火墙

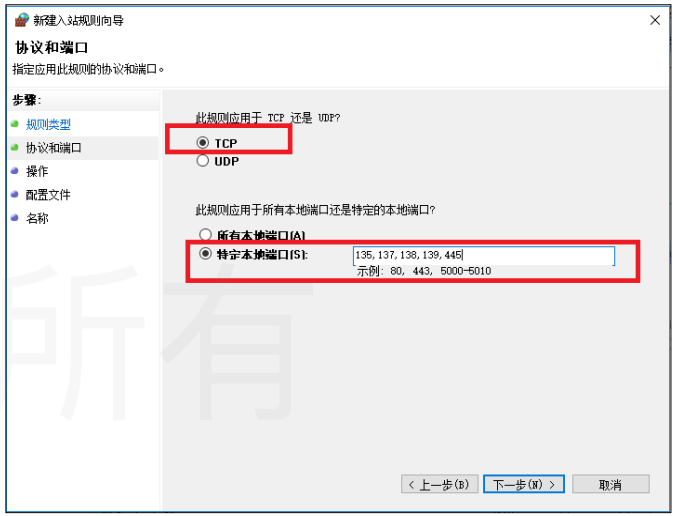
- 点击“开始”，然后单击“控制面板”；
- 点击“Windows 防火墙”，针对Windows 防火墙进行配置；
- 点击"打开或关闭Windows 防火墙"，定义每种类型网络的防火墙设置；
- 针对专用网络或公用网络，打开或关闭Windows 防火墙；
- 点击“高级设置”>>入站规则>>新建规则；
- 选择端口，下一步；
- 在特定本地端口，输入需要关闭的端口号445,135,137,138,139，下一步；
- 选择阻止连接，下一步；
- 配置文件，全选，下一步；
- 名称，可以任意输入，完成即可。

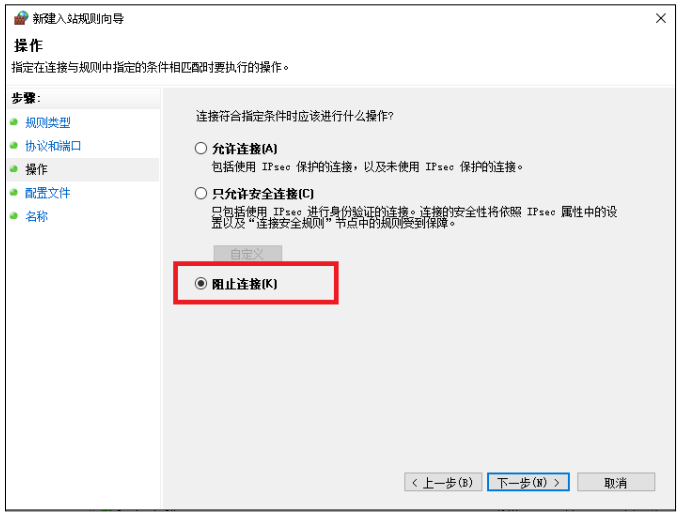
远程代码执行漏洞(MS17-010)加固

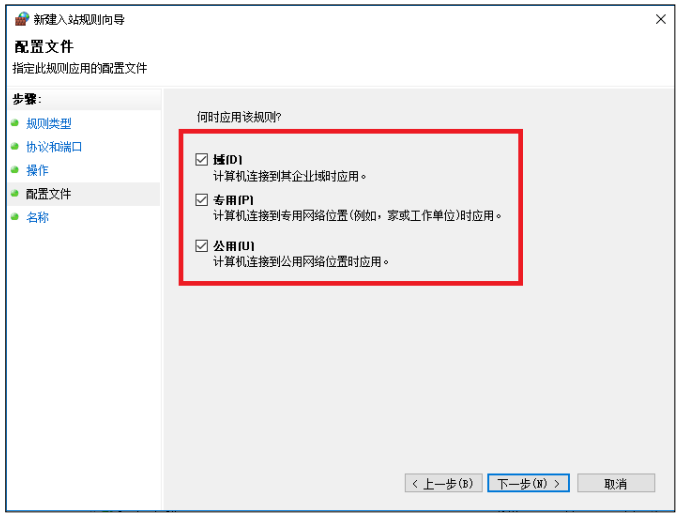
通过开启防火墙功能，阻止访问受影响的445端口。同时，可以设置白名单，允许受信的主机访问。

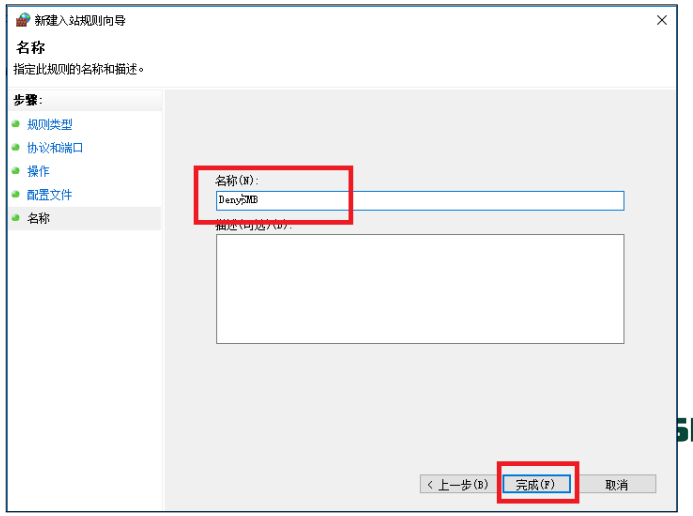












2.2

SSH漏洞加固方案

SSH漏洞加固

启动会

① 对安全加固活动进行宣讲

② 落实服务所需的人员、设备、资料等资源

实施加固计划

① 明确的项目组织及职责；

② 明确的项目实施阶段各项工作任务的内容及要求，以及工程和环节的逻辑顺序；

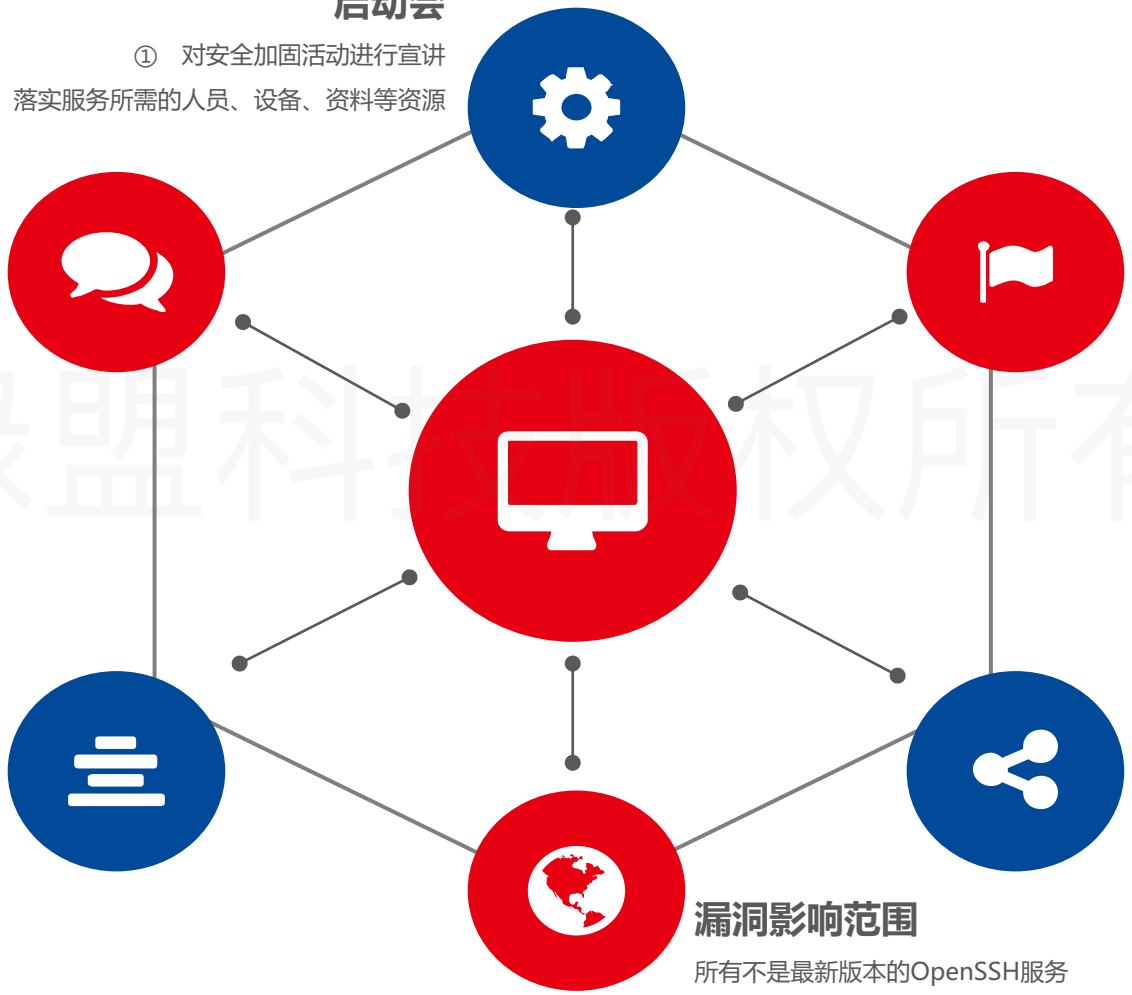
③ 编制分时间阶段的实施进度表，使所有工作任务正确地定位并考虑完成每项任务有充分的时间；

④ 确定每项任务需要的资源，以保证项目实施时期获得足够的支持；

⑤ 将所有实施数据计入文件，以便使实施计划能做出及时修订。

实施加固清单

明确项目范围内的系统资产存在漏洞的IP地址



漏洞描述

① OpenSSH 是一组用于安全地访问远程计算机的连接工具， 对所有的传输进行加密。

② 由于OpenSSH版本过低，导致出现比较多的高、中风险漏洞。

漏洞威胁

OpenSSH版本漏洞，攻击者可执行任意代码，提升权限至root权限，获取本地敏感信息泄露，绕过某些安全限制执行未经授权的操作。

漏洞影响范围

所有不是最新版本的OpenSSH服务

NSFOCUS

SSH漏洞加固

加固方案：1. 安装最新SSH版本

先决条件

- 准备升级OpenSSH及其所依赖的openssl升级包 (gcc、openssh-7.9p1.tar.gz、openssl-1.0.2q.tar.gz、zlib-1.2.11.tar、pam-devel-1.1.1-24.el6.x86_64.rpm)

操作步骤

- 临时开启telnet远程登录方式
- OpenSSH版本升级
  - ✓ 卸载原openssh
  - ✓ 编译安装gcc
  - ✓ 升级Zlib
  - ✓ 更新PAM
  - ✓ 编译安装openssl
  - ✓ 编译安装OpenSSH
  - ✓ 重启OpenSSH
  - ✓ 查看OpenSSH版本，确认升级成功
- 关闭telnet远程登录方式

openssh依赖的软件	状态	说明
Zlib	**必选**	用于提供压缩和解压缩功能
libcrypto (LibreSSL或OpenSSL)	**必选**	OpenSSH依赖于libcrypto，而libcrypto可以由LibreSSL或OpenSSL提供。
PAM	**可选**	用于提供安全控制

SSH漏洞加固

Linux中openssh漏洞修复步骤详解

备份启动脚本

cp /etc/init.d/sshd /root/

停止SSHD服务

/sbin/service sshd stop

卸载系统里原有Openssh

rpm -qa|grep openssh //查询系统原安装的openssh包,全部卸载。
rpm -e openssh --nodeps
rpm -e openssh-server --nodeps
rpm -e openssh-clients --nodeps
rpm -e openssh-askpass
或rpm -e --nodeps `rpm -qa |grep openssh`

```
[root@gw OpenSSL]# tar -xvf openssl-1.0.2q.tar.gz
[root@gw OpenSSL]# cd openssl-1.0.2q
[root@gw openssl-1.0.2q]# ./config --prefix=/opt/openssl1.0.2q _20170617 --openssldir=/opt/openssl1.0.2q_2017061
7/openssl fips --with-fipsdir=/opt/fips-2.0.16 zlib-dynamic shared -fPIC
[root@gw openssl-1.0.2q]# make depend
[root@gw openssl-1.0.2q]# make
[root@gw openssl-1.0.2q]# make test
[root@gw openssl-1.0.2q]# make install
```

```
# tar  - jxvf zlib-1.2.11.tar.bz2 //首先安装zlib库，否则会报zlib.c错误无法进行
# cd zlib-1.2.11
# ./configure
# make&&make install
```

```
[root@gw OpenSSH]# tar -xvf openssh-7.9p1.tar.gz
[root@gw OpenSSH]# cd openssh-7.9p1
[root@gw openssh-7.9p1]# ./configure --prefix=/opt/openssh7.9.p1_20170617 --with-ssl-dir=/opt/openssl1.0.2q_201
70617 --with-pam
[root@gw openssh-7.9p1]# make
[root@gw openssh-7.9p1]# make install
```

```
[root@gw ~]# service sshd restart
```

```
[root@localhost ~]# rpm -ivh pam-devel-1.1.1-24.el6.x86_64.rpm
Preparing...                ########################################### [100%]
   1:pam-devel              ########################################### [100%]
```

```
[root@gw ~]# ssh -V
OpenSSH_7.9p1, OpenSSL 1.0.2q-fips  25 Dec 2018
```

SSH漏洞加固

- **加固方案：2. 在防火墙处阻止SSH端口**

```
root@kali:~# iptables -L    //查看本机IPTABLES的设置情况
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@kali:~#  iptables -I INPUT -p tcp --dport 22 -j DROP //拒绝所有非信任主机的远程SSH登陆
root@kali:~#  iptables -I INPUT -s 192.168.88.73 -p tcp --dport 22 -j ACCEPT //允许4A、堡垒机等可信主机访问
root@kali:~#  iptables -I OUTPUT -p tcp --sport 22 -j ACCEPT //如果OUTPUT 设置成DROP，就要写上这一条
root@kali:~#  iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.88.73        anywhere             tcp dpt:ssh
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp spt:ssh
root@kali:~# service iptables save    //保存规则
root@kali:~# service iptables restart   //重启iptables
```

03

常见数据库漏洞加固

1. TNS劫持漏洞加固方案
2. 数据库高危漏洞加固方案

NSFOCUS

3.1

TNS劫持漏洞加固方案

数据库'TNS Listener'远程数据投毒漏洞加固

启动会

① 对安全加固活动进行宣讲

② 落实服务所需的人员、设备、资料等资源

实施加固计划

① 明确的项目组织及职责；

② 明确的项目实施阶段各项工作任务的内容及要求，以及工程和环节的逻辑顺序；

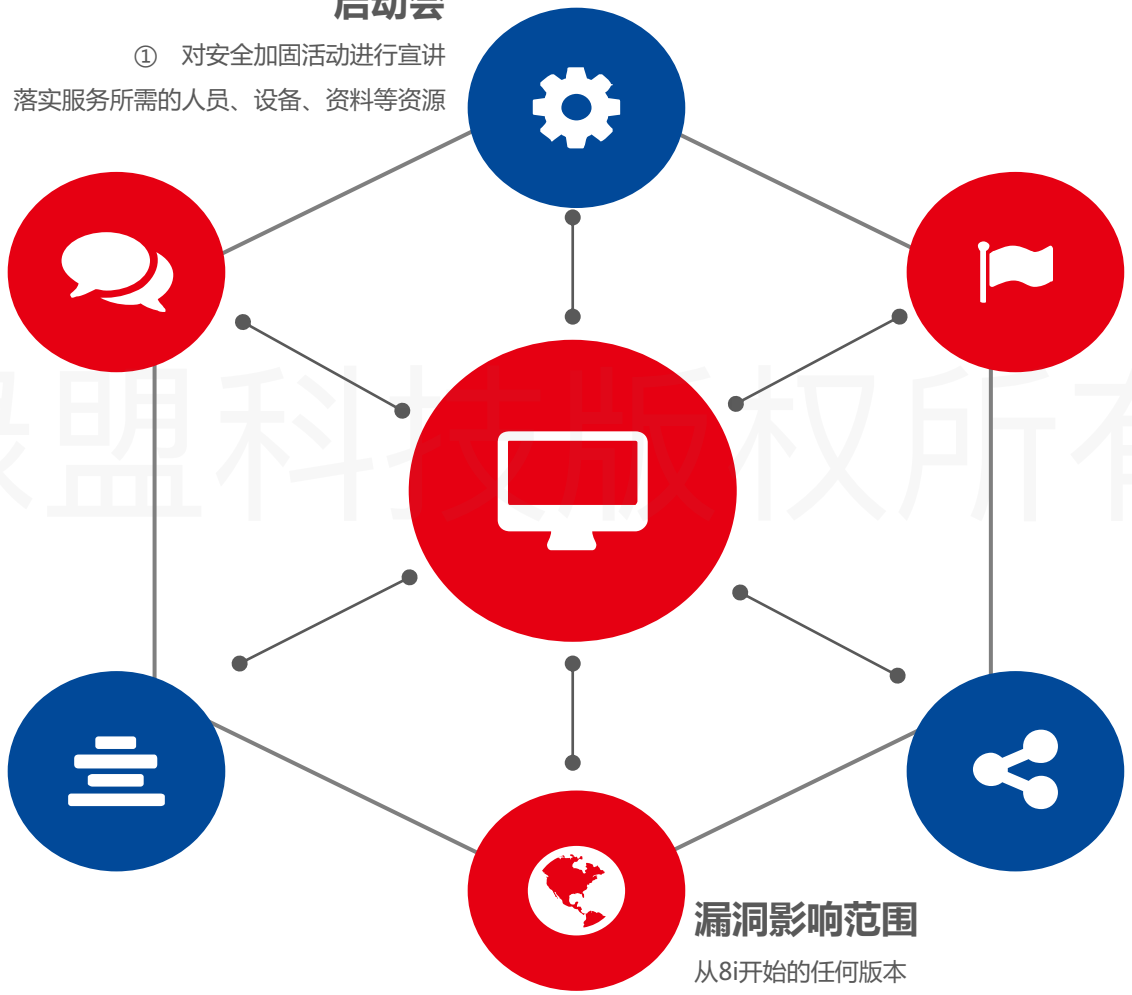
③ 编制分时间阶段的实施进度表，使所有工作任务正确地定位并考虑完成每项任务有充分的时间；

④ 确定每项任务需要的资源，以保证项目实施时期获得足够的支持；

⑤ 将所有实施数据计入文件，以便使实施计划能做出及时修订。

实施加固清单

明确项目范围内的系统资产存在漏洞的IP地址



漏洞影响范围

从8i开始的任何版本

漏洞描述

① Oracle Database Server是一个对象一关系数据库管理系统。

② Oracle Database Server在实现上存在可允许攻击者向远程'TNS Listener'组件处理的数据投毒的漏洞，攻击者无需用户名和密码可利用此漏洞将数据库服务器的合法'TNS Listener'组件中的数据转向到攻击者控制的系统，导致控制远程组件的数据库实例，造成组件和合法数据库之间的攻击者攻击、会话劫持或拒绝服务攻击。

漏洞威胁

攻击者可以自行创建一个和当前生产数据库同名的数据库，将其向生产数据库的监听注册。这样将导致用户连接被路由指向攻击者创建的实例，造成业务响应中断

NSFOCUS

数据库'TNS Listener'远程数据投毒漏洞加固

加固方案： 1. 限制注册本地实例

先决条件

- 做好数据库的备份和恢复有效性的测试

操作步骤

- 查看数据库 ‘TNS Listener’ 的配置文件和监听信息
- 安装patch12880299
- 在listener.ora增加"SECURE_REGISTER_LISTENER_PROD = (TCP)“
- 重启Listener监听
- 查看listener.log日志，会出现TNS-01194拒绝注册的信息

数据库'TNS Listener'远程数据投毒漏洞加固

Oracle数据库'TNS Listener'漏洞修复步骤详解

```
# listener.ora Network Configuration File: [redacted]\listener.ora
# Generated by Oracle configuration tools.
LISTENER =
(DESCRIPTION_LIST =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
(ADDRESS = (PROTOCOL = TCP)(HOST = [redacted])(PORT = 1521))
)
)
SID_LIST_LISTENER =
(SID_LIST =
(SID_DESC =
(SID_NAME = PLSExtProc)
(ORACLE_HOME = [redacted]\db_1)
(PROGRAM = extproc)
(ENVS = "EXTPROC_DLLS=ANY")
)
(SID_DESC =
(GLOBAL = orcl)
(ORACLE_HOME = [redacted]\db_1)
(SID_NAME = orcl)
)
)
ADR_BASE_LISTENER = [redacted]racle
```

查看oracle监听配置文件listener.ora

```
SQL> show parameter local_listener
NAME TYPE VALUE
------------------------------------ ----------- ------------------------
local_listener string
SQL> show parameter remote_listener;
NAME TYPE VALUE
------------------------------------ ----------- ------------------------
remote_listener string
SQL>
```

查看数据库监听信息

```
$ opatch prereq CheckConflictAgainstOHWithDetail -phBaseDir ./12880299
$ cd 12880299
$ opatch apply
```

冲突性检查，安装patch:12880299

```
$ opatch lsinventory | grep 12880299
```

检查是否安装成功

```
LISTENER_PROD =
  (DESCRIPTION_LIST =
   (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = netfl-bde)(PORT = 1551))
   )
  )

SECURE_REGISTER_LISTENER_PROD = (TCP)
```

在listener.ora增加 "SECURE_REGISTER_listener_name = (TCP) "

```
$ lsnrctl stop listener_prod
$ lsnrctl start lintener_prod
```

重启'TNS Listener服务

```
[oracle@bde]$ tail /u01/app/oracle/product/11.2.0.2/network/log/listener.log


04-MAY-2012 10:43:03 * (CONNECT_DATA=(CID=(PROGRAM=)(HOST=netfl-bde)(USER=oracle))
(COMMAND=services)(ARGUMENTS=64)(SERVICE=LISTENER)(VERSION=186647040)) * services * 0

04-MAY-2012 10:43:05 * service_register_NSGR * 1194
TNS-01194: The listener command did not arrive in a secure transport

04-MAY-2012 10:44:05 * service_register_NSGR * 1194
TNS-01194: The listener command did not arrive in a secure transport
```

查看listener日志，会出现TNS-01194拒绝注册的信息

数据库'TNS Listener'远程数据投毒漏洞加固

加固方案： 2. 限制数据库注册本地实例

先决条件

- 做好数据库的备份

操作步骤

- 查看数据库 ‘TNS Listener’ 的配置文件和监听信息
- 关停Listener监听
- 在listener.ora增加"SECURE_REGISTER_LISTENER_PROD = (IPC)“
- 启动Listener监听
- 修改local_listener参数
- 查看listener.log日志，会出现TNS-01194拒绝注册的信息

数据库'TNS Listener'远程数据投毒漏洞加固

Oracle数据库'TNS Listener'漏洞修复步骤详解

```
# listener.ora Network Configuration File: [redacted]\listener.ora
# Generated by Oracle configuration tools.
LISTENER =
(DESCRIPTION_LIST =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
(ADDRESS = (PROTOCOL = TCP)(HOST = [redacted])(PORT = 1521))
)
)
SID_LIST_LISTENER =
(SID_LIST =
(SID_DESC =
(SID_NAME = PLSExtProc)
(ORACLE_HOME = [redacted]\db_1)
(PROGRAM = extproc)
(ENVS = "EXTPROC_DLLS=ANY")
)
(SID_DESC =
(GLOBAL = orcl)
(ORACLE_HOME = [redacted]\db_1)
(SID_NAME = orcl)
)
)
ADR_BASE_LISTENER = [redacted]racle
```

查看oracle监听配置文件listener.ora

```
SQL> show parameter local_listener
NAME TYPE VALUE
------------------------------------ ----------- ------------------------
local_listener string
SQL> show parameter remote_listener;
NAME TYPE VALUE
------------------------------------ ----------- ------------------------
remote_listener string
SQL>
```

查看数据库监听信息

```
$ lsnrctl stop listener_prod
```

关停Listener监听

```
LISTENER.ORA
------------
LISTENER_PROD =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = IPC)(KEY = REGISTER))
      (ADDRESS = (PROTOCOL = TCP)(HOST = netfl-bde)(PORT = 1551))
    )
  )

SECURE_REGISTER_LISTENER_PROD = (IPC)
```

在listener.ora增加"SECURE_REGISTER_LISTENER_PROD = (IPC)"

```
$ lsnrctl start lintener_prod
```

启动Listener监听

```
SQL> alter system set local_listener='(DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=REGISTER)))' scope = both;

System altered.


SQL> show parameter local_listener

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
local_listener                       string      (DESCRIPTION=(ADDRESS=(PROTOCO
                                                 L=IPC)(KEY=REGISTER)))
```

修改local_listener参数

```
[oracle@bde]$ tail /u01/app/oracle/product/11.2.0.2/network/log/listener.log


04-MAY-2012 10:43:03 * (CONNECT_DATA=(CID=(PROGRAM=)(HOST=netfl-bde)(USER=oracle))
(COMMAND=services)(ARGUMENTS=64)(SERVICE=LISTENER)(VERSION=186647040)) * services * 0

04-MAY-2012 10:43:05 * service_register_NSGR * 1194
TNS-01194: The listener command did not arrive in a secure transport

04-MAY-2012 10:44:05 * service_register_NSGR * 1194
TNS-01194: The listener command did not arrive in a secure transport
```

查看listener日志，会出现TNS-01194拒绝注册的信息

3.2

数据库高危漏洞加固方案

数据库高危漏洞加固

启动会

① 对安全加固活动进行宣讲

② 落实服务所需的人员、设备、资料等资源

实施加固计划

① 明确的项目组织及职责；

② 明确的项目实施阶段各项工作任务的内容及要求，以及工程和环节的逻辑顺序；

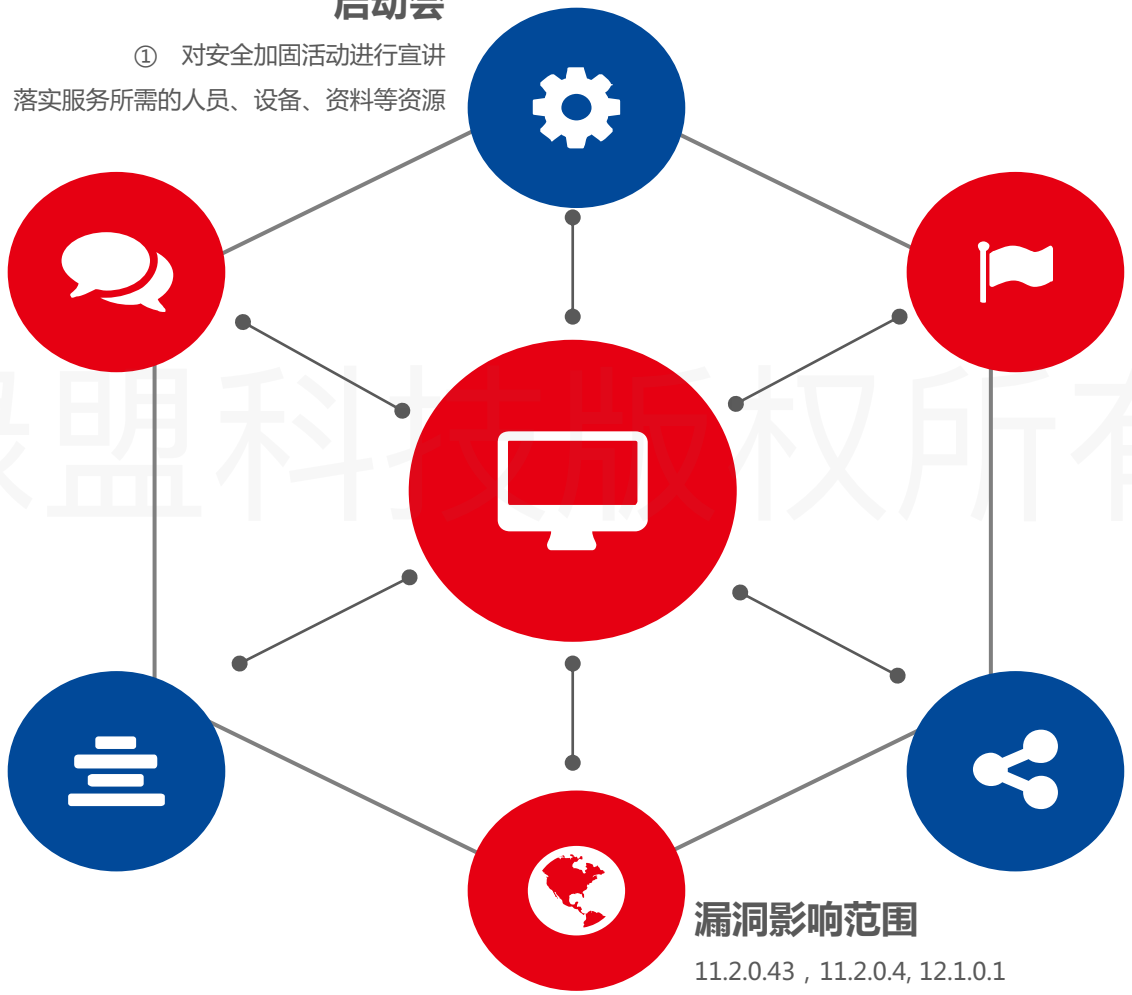
③ 编制分时间阶段的实施进度表，使所有工作任务正确地定位并考虑完成每项任务有充分的时间；

④ 确定每项任务需要的资源，以保证项目实施时期获得足够的支持；

⑤ 将所有实施数据计入文件，以便使实施计划能做出及时修订。

实施加固清单

明确项目范围内的系统资产存在漏洞的IP地址



漏洞描述

① Oracle Database Server是一个对象一关系数据库管理系统。

② Oracle Database Server在RDBMS Core组件的实现上存在远程安全漏洞，此漏洞可通过Oracle Net协议利用，经过身份验证的远程攻击者可利用此漏洞影响受影响组件的机密性。

漏洞威胁

仅有查询权限的用户可以对数据进行增、删、改操作，非常危险

漏洞影响范围

11.2.0.43，11.2.0.4, 12.1.0.1

NSFOCUS

数据库高危漏洞加固

加固方案： 安装PSU补丁

先决条件

- 做好数据库的备份和恢复有效性的测试

操作步骤

- 查看当前使用的数据库版本
- 关停数据库实例和监听，并确认无相关进程
- 检查补丁冲突
- 通过opatch安装PSU补丁
- 重启数据库实例和监听
- 更新数据库数据字典
- 检查补丁是否安装成功

数据库高危漏洞加固

Oracle数据库补丁安装步骤详解

```
[oracle@orcl11204 20299013]$ opatch prereq CheckConflictAgainstOHWithDetail -ph ./
Oracle Interim Patch Installer version 11.2.0.3.4
Copyright (c) 2012, Oracle Corporation.  All rights reserved.
PREREQ session
Oracle Home       : /opt/oracle/product/11.2.0.4/db
Central Inventory : /opt/oraInventory
   from           : /opt/oracle/product/11.2.0.4/db/oraInst.loc
OPatch version    : 11.2.0.3.4
OUI version       : 11.2.0.4.0
Log file location : /opt/oracle/product/11.2.0.4/db/cfgtoollogs/opatch/opatch2015-06-29_17-46-33PM_1.log
Invoking prereq "checkconflictagainstohwithdetail"
Prereq "checkConflictAgainstOHWithDetail" passed.
OPatch succeeded.
```

检查补丁冲突

```
[oracle@orcl11204 20299013]$ opatch apply
Oracle Interim Patch Installer version 11.2.0.3.11
Copyright (c) 2015, Oracle Corporation.  All rights reserved.
Oracle Home       : /opt/oracle/product/11.2.0.4/db
Central Inventory : /opt/oraInventory
   from           : /opt/oracle/product/11.2.0.4/db/oraInst.loc
OPatch version    : 11.2.0.3.11
OUI version       : 11.2.0.4.0
Log file location : /opt/oracle/product/11.2.0.4/db/cfgtoollogs/opatch/opatch2015-06-29_18-53-23PM_1.log
Trace Level               on
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File   /opt/oracle/product/11.2.0.4/db/network/admin/listener.ora
Listener Log File         /opt/oracle/diag/tnslsnr/orcl11204/listener/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=orcl11204)(PORT=1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
The listener supports no services
The command completed successfully
[oracle@orcl11204 20299013]$ ps -ef|grep ora_
oracle    1757 24201  0 17:51 pts/2    00:00:00 grep ora_
```

安装PSU补丁

```
[oracle@orcl11204 20299013]$ sqlplus / as sysdba
SQL*Plus: Release 11.2.0.4.0 Production on Mon Jun 29 19:08:09 2015
Copyright (c) 1982, 2013, Oracle.  All rights reserved.
Connected to an idle instance.
SQL> startup
ORACLE instance started.
Total System Global Area  726540288 bytes
Fixed Size    2256792 bytes
Variable Size  478150760 bytes
Database Buffers  243269632 bytes
Redo Buffers    2863104 bytes
Database mounted.
Database opened.
```

重启数据库

```
[oracle@orcl11204 20299013]$ opatch lsinventory
Oracle Interim Patch Installer version 11.2.0.3.11
Copyright (c) 2015, Oracle Corporation.  All rights reserved.
Oracle Home       : /opt/oracle/product/11.2.0.4/db
Central Inventory : /opt/oraInventory
   from           : /opt/oracle/product/11.2.0.4/db/oraInst.loc
OPatch version    : 11.2.0.3.11
OUI version       : 11.2.0.4.0
Log file location : /opt/oracle/product/11.2.0.4/db/cfgtoollogs/opatch/opatch2015-06-29_19-07-44PM_1.log
Lsinventory Output file location : /opt/oracle/product/11.2.0.4/db/cfgtoollogs/opatch/lsinv/lsinventory2015-06-29_19-07-44PM.txt
--------------------------------------------------------------------------------
Local Machine Information::
Hostname: orcl11204
ARU platform id: 226
ARU platform description:: Linux x86-64
Installed Top-level Products (1):
Oracle Database 11g                                  11.2.0.4.0
There are 1 products installed in this Oracle Home.
Interim patches (1) :
Patch  20299013     : applied on Mon Jun 29 19:00:43 CST 2015
Unique Patch ID:  18573940
Patch description:  "Database Patch Set Update : 11.2.0.4.6 (20299013)"
```

检查补丁是否安装成功

04

常见中间件漏洞加固

1. Struts2漏洞加固方案
2. 反序列化漏洞加固方案

NSFOCUS

4.1

Struts2漏洞加固方案

Struts2 s2-057漏洞加固

启动会

① 对安全加固活动进行宣讲

② 落实服务所需的人员、设备、资料等资源

实施加固计划

① 明确的项目组织及职责；

② 明确的项目实施阶段各项工作任务的内容及要求，以及工程和环节的逻辑顺序；

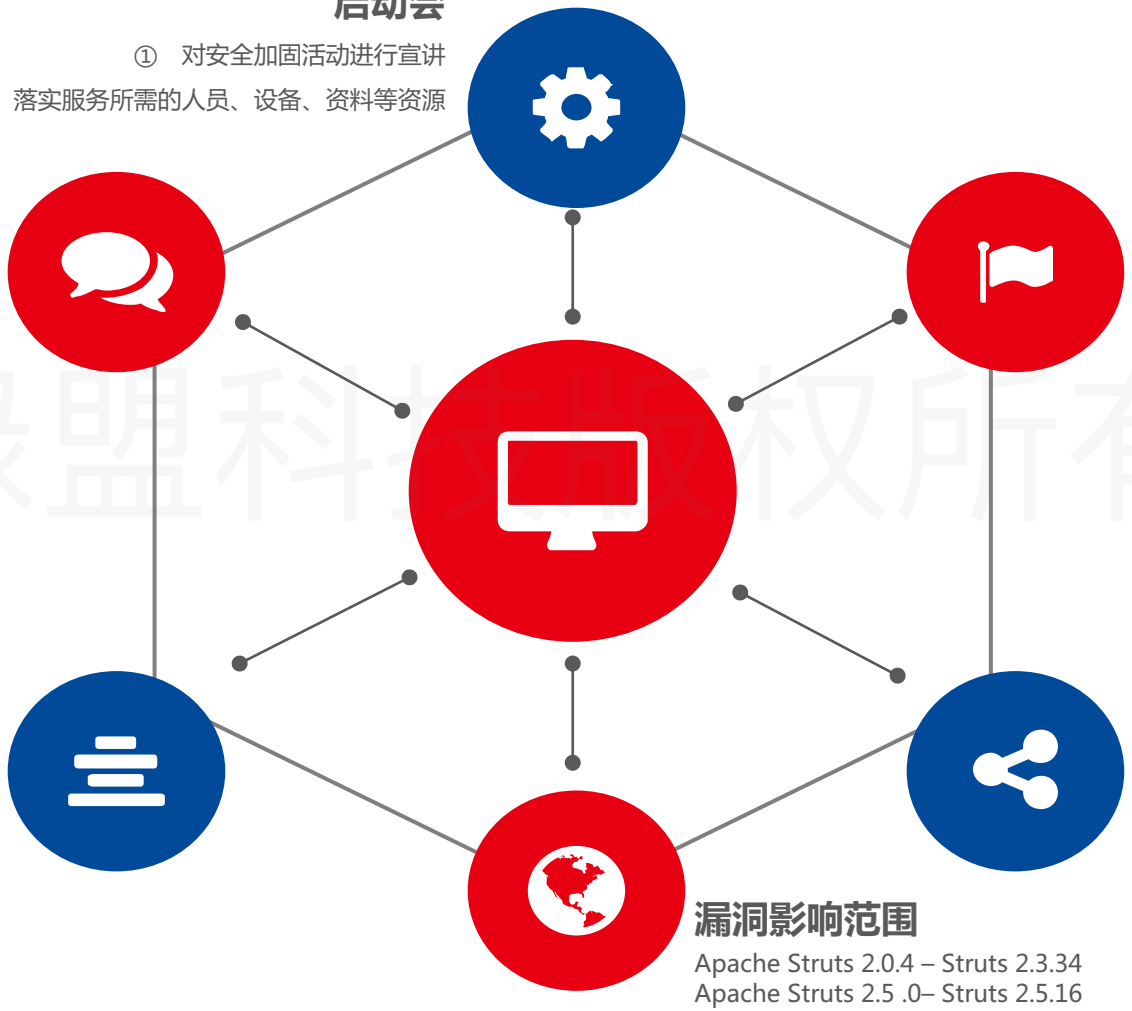
③ 编制分时间阶段的实施进度表，使所有工作任务正确地定位并考虑完成每项任务有充分的时间；

④ 确定每项任务需要的资源，以保证项目实施时期获得足够的支持；

⑤ 将所有实施数据计入文件，以便使实施计划能做出及时修订。

实施加固清单

明确项目范围内的系统资产存在漏洞的IP地址



漏洞描述

① Struts2整合了动态网站技术中Srvlet、JSP、JavaBean、JDBC、XML等相关开发技术基础之上的一种WEB开发框架，是一个基于MVC设计模式的Web应用框架。

② 在Struts2开发框架中使用namespace功能定义XML配置时，namespace值未被设置且在上层动作配置（Action Configuration）中未设置或用通配符namespace，可能导致远程代码执行。同理，url标签未设置value和action值且上层动作未设置或用通配符namespace时也可能导致远程代码执行

漏洞威胁

实际场景中存在一定局限性，需要满足一定条件。

漏洞影响范围

Apache Struts 2.0.4 – Struts 2.3.34
Apache Struts 2.5 .0– Struts 2.5.16

NSFOCUS

Struts2 s2-057漏洞加固

- **加固方案：1. 将Struts2升级至官方修复版本，2.3.*的用户请升级至2.3.35；2.5.*的用户请升级至2.5.17**
  - **先决条件**
    - 确定Struts2升级目标版本所需的基本依赖包
    - 做好WEB项目的备份
  - **操作步骤**
    - 判断当前使用的struts2版本
    - 将下载的jar包替换WEB项目WEB-INF/lib目录下面相应的jar包　//将上个版本相应的jar删除，替换成最新的

Struts2 s2-057漏洞加固

struts2漏洞修复步骤详解

root@localhost:~

File Edit View Search Terminal Help

判断当前Struts2版本

```
[root@localhost ~]# find / -name struts2-core-*.jar
/root/Documents/struts-2.3.32/lib/struts2-core-2.3.32.jar
[root@localhost ~]#
```

commons-fileupload-1.3.2.jar	2018/7/24 11:18	Executable Jar File	69 KB
commons-io-2.2.jar	2018/7/24 9:11	Executable Jar File	170 KB
commons-lang3-3.2.jar			376 KB
commons-logging-1.1.3.jar	2018/7/24 10:58	Executable Jar File	61 KB
freemarker-2.3.28.jar	2018/7/24 11:18	Executable Jar File	1,489 KB
javassist-3.11.0.GA.jar	2018/7/24 10:58	Executable Jar File	600 KB
ognl-3.0.21.jar	2018/7/24 10:58	Executable Jar File	226 KB
struts2-core-2.3.35.jar	2018/7/24 11:49	Executable Jar File	885 KB
xwork-core-2.3.35.jar	2018/7/24 11:48	Executable Jar File	695 KB

下载的jar包替换WEB项目WEB-INF/lib目录中对应的文件

Index of /dist/struts/2.3.35

Name	Last modified	Size	Description
Parent Directory		-	
struts-2.3.35-all.zip	2018-08-11 16:33	79M	
struts-2.3.35-all.zip.asc	2018-08-11 16:33	827	
struts-2.3.35-all.zip.md5	2018-08-11 16:33	32	
struts-2.3.35-all.zip.sha1	2018-08-11 16:33	40	
struts-2.3.35-apps.zip	2018-08-11 16:33	39M	
struts-2.3.35-apps.zip.asc	2018-08-11 16:33	827	
struts-2.3.35-apps.zip.md5	2018-08-11 16:33	32	
struts-2.3.35-apps.zip.sha1	2018-08-11 16:33	40	
struts-2.3.35-docs.zip	2018-08-11 16:33	11M	
struts-2.3.35-docs.zip.asc	2018-08-11 16:33	827	
struts-2.3.35-docs.zip.md5	2018-08-11 16:33	32	
struts-2.3.35-docs.zip.sha1	2018-08-11 16:33	40	
struts-2.3.35-lib.zip	2018-08-11 16:33	21M	
struts-2.3.35-lib.zip.asc	2018-08-11 16:33	827	
struts-2.3.35-lib.zip.md5	2018-08-11 16:33	32	
struts-2.3.35-lib.zip.sha1	2018-08-11 16:33	40	
struts-2.3.35-min-lib.zip	2018-08-11 16:33	4.0M	
struts-2.3.35-min-lib.zip.asc	2018-08-11 16:33	827	
struts-2.3.35-min-lib.zip.md5	2018-08-11 16:33	32	

更新下载基本依赖包即可

Struts2 s2-057漏洞加固

- **加固方案：2. 排查所有Struts 2的配置文件，如struts.xml，为没有定义namespace命名空间的package节点添加命名空间配置。**

```
<package name="user" namespace="/user" extends="struts-default">
    <action name="login">
    </action>
</package>
```

Struts2 s2-057漏洞加固

- **加固方案：3. 使用防护类产品定制策略进行防护。**

4.2

反序列化漏洞加固方案

Weblogic远程代码执行漏洞CVE-2018-3245加固

启动会

① 对安全加固活动进行宣讲

② 落实服务所需的人员、设备、资料等资源

实施加固计划

① 明确的项目组织及职责；

② 明确的项目实施阶段各项工作任务的内容及要求，以及工程和环节的逻辑顺序；

③ 编制分时间阶段的实施进度表，使所有工作任务正确地定位并考虑完成每项任务有充分的时间；

④ 确定每项任务需要的资源，以保证项目实施时期获得足够的支持；

⑤ 将所有实施数据计入文件，以便使实施计划能做出及时修订。

实施加固清单

明确项目范围内的系统资产存在漏洞的IP地址

漏洞影响范围

Oracle WebLogic Server10.3.6.0
Oracle WebLogic Server12.2.1.3
Oracle WebLogic Server12.1.3.0

漏洞描述

① WebLogic Server 中的 RMI 通信使用 T3 协议在 WebLogic Server和其他 Java程序（包括客户端及其他 WebLogic Server 实例）间传输数据（序列化的类）。由于WebLogic的T3协议和Web协议共用同一个端口，因此只要能访问WebLogic就可利用T3协议实现payload和目标服务器的通信。

② WebLogic java反序列化漏洞（CVE-2018-3245）是通过JRMP协议利用RMI机制的缺陷，进行远程代码执行漏洞的利用。攻击者可以在未授权的情况下，将payload封装，并通过WebLogic的T3协议进行传输，通过对T3协议中的payload进行反序列化，实现对存在漏洞的WebLogic组件进行远程攻击。实现任意代码执行，并获取目标系统的所有权限。

漏洞威胁

攻击者可以在未授权的情况下将payload封装在T3协议中，通过对T3协议中的payload进行反序列化，从而实现对存在漏洞的WebLogic组件进行远程攻击，执行任意代码并可获取目标系统的所有权限。

NSFOCUS

Weblogic远程代码执行漏洞CVE-2018-3245加固

加固方案：1. Weblogic官方CPU更新补丁

先决条件

- 确定补丁类型，不同补丁类型有不同安装方法
- 确定weblogic版本，以及它已经安装的补丁集
- 一定要查看oracle给出的README补丁说明文件（补丁压缩包中会附带）
- 补丁安装前做好WLS_HOME备份

操作步骤

- 判断当前使用的weblogic版本
- 停止weblogic服务，并确认无相关进程
- 将补丁包p28343311_1036_Generic.zip上传到weblogic指定的目录
- 将补丁包p28343311_1036_Generic.zip解压
- 修改bsu.sh脚本，将内存调大，解决内存溢出的问题
- 执行bsu.sh安装命令
- 重启WebLogic，检查补丁包是否安装成功

Weblogic远程代码执行漏洞CVE-2018-3245加固

Weblogic远程代码执行漏洞修复步骤详解

```
[root@app1 bsu]$ cd /wls11g/wlserver_10.3/server/bin/

[root@app1 bin]$ source setWLSEnv.sh > /dev/null

[root@app1 bin]$ java weblogic.version        查看weblogic版本

WebLogic Server 10.3.6.0Tue Nov 15 08:52:36 PST 2011 1441050

Use 'weblogic.version -verbose' to getsubsystem information

Use 'weblogic.utils.Versions' to getversion information for all modules
```

```
[root@app1 cache_dir]# unzip p28343311_1036_Generic.zip
Archive:  p28343311_1036_Generic.zip          将补丁包解压
 extracting: GENM.jar
  inflating: patch-catalog_26256.xml
  inflating: README.txt
```

```
root@app1 bsu]# ./bsu.sh -install -patch_download_dir=/wls11g/utils/bsu/cache_di
-prod_dir=/wls11g/wlserver_10.3                安装补丁
Checking for conflicts.....................
No conflict(s) detected
Installing Patch ID: GENM..
Result: Success
```

```
[root@app1 bsu]# ./bsu.sh -prod_dir=/wls11g/wlserver_10.3 -status=applied -verbose -view
ProductName:       WebLogic Server                检查补丁包是否安装成功
ProductVersion:    10.3 MP6
Components:        WebLogic Server/Core Application Server,WebLogic Server/Admi
                   nistration Console,WebLogic Server/Configuration Wizard and
                   Upgrade Framework,WebLogic Server/Web 2.0 HTTP Pub-Sub Serve
                   r,WebLogic Server/WebLogic SCA,WebLogic Server/WebLogic JDBC
                    Drivers,WebLogic Server/Third Party JDBC Drivers,WebLogic S
                   erver/WebLogic Server Clients,WebLogic Server/WebLogic Web S
                   erver Plugins,WebLogic Server/UDDI and Xquery Support,WebLog
                   ic Server/Evaluation Database,WebLogic Server/Workshop Code
                   Completion Support
BEAHome:           /wls11g
ProductHome:       /wls11g/wlserver_10.3
PatchSystemDir:    /wls11g/utils/bsu
PatchDir:          /wls11g/patch_wls1036
Profile:           Default
DownloadDir:       /wls11g/utils/bsu/cache_dir
JavaVersion:       1.6.0_29
JavaVendor:        Sun
Patch ID:          GENM
PatchContainer:    GENM.jar
Checksum:          -345780037
Severity:          optional
Category:          General
CR/BUG:            28343311
Restart:           true
Description:       WLS PATCH SET UPDATE 10.3.6.0.181016
WLS PATCH SET UPDATE 10.3.6.0.181016
```


NSFOCUS

Weblogic远程代码执行漏洞CVE-2018-3245加固

加固方案：2. 对t3及t3s协议进行访问控制

先决条件

- WebLogic Server和其他 Java程序（包括WebLogic Server 实例）使用 T3 协议的IP地址。

操作步骤

- 进入WebLogic控制台，在base_domain的配置页面中，进入“安全”选项卡页面，点击“筛选器”，进入连接筛选器配置。
- 在连接筛选器中输入：weblogic.security.net.ConnectionFilterImpl，在连接筛选器规则中输入：127.0.0.1 * * allow t3 t3s，0.0.0.0/0 * * deny t3 t3s（t3和t3s协议的所有端口只允许本地访问）。
- 保存后需重新启动，规则方可生效。

Weblogic远程代码执行漏洞CVE-2018-3245加固

此漏洞产生于WebLogic的T3服务，因此可通过控制T3协议的访问来临时阻断针对该漏洞的攻击。

NSFOCUS

05

常见加固问题及处理方法

NSFOCUS

常见问题及处理方法

问题一：运维人员和安全人员双方，因关注点不同而导致的分歧

安全人员

- 关注如何按时完成漏洞的修复

运维人员

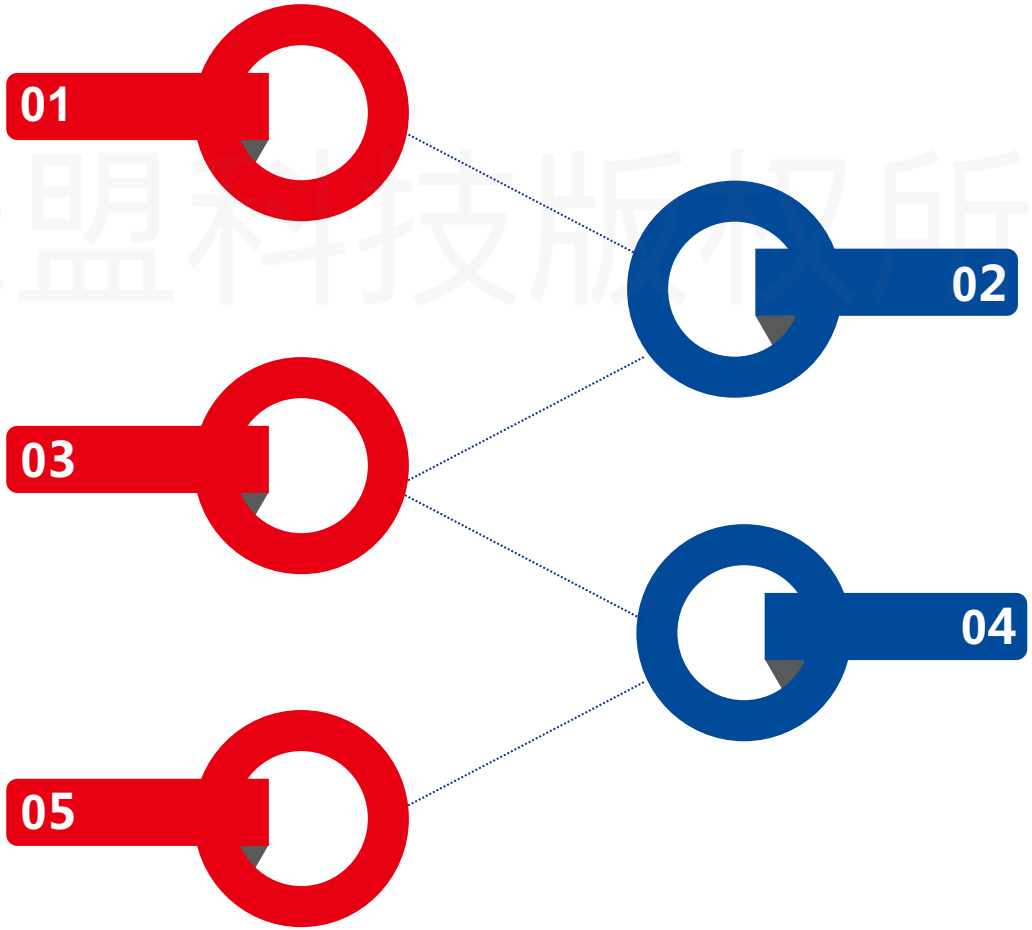
- 加固是否会影响业务系统的正常运行
- 加固是否会带来业务上的中断。
- 加固是否会给系统带来性能上的影响。
- 加固实施是否会带来大量的工作量和挤占大量的时间。
- 加固后运维工作是否会在操作上十分不便。
- 加固后的主机是否会在安全上和现有水平相比，有很大提升。

常见问题及处理方法

分歧的处理

主要矛盾是相关人员对加固没有了解，不清楚项目可能会带来哪些“利”、“弊。可以通过会议的方式，向各个部门的Leader ，骨干进行加固方面的知识介绍和内容宣讲。

为了验证自身说法的科学性，前期测试需要通过数据证明各种影响的具体数值，并给出目前的数值进行比较。根据数据同运维线沟通，商讨性能等指标容忍基线。



方案在设计时要充分考虑业务中断、性能的影响。在初始设计上规避重起等可能造成中断的行为，并出具了性能评估报告，比较图谱等进行性能影响验证。为了使报告具有说服力，应尽量争取将被运维部门提供样机，以便采集数据得到较大范围的认可。

采取自动化脚本、程序的模式进行。事先设置好加固项的配置文件后，执行安装脚本自动化部署，尽量避免部署所带来的时间和人力成本。

提供一份加固影响表，将每项加固内容可能带来的影响进行描述，并且在实施中时时更新此表，并同步收集故障案例，作为培训资料。

加固效果的验证本身存在一定的困难，前期可以采用制作PPT讲解等方式，后期进行培训时，可以构建一些演练环境进行展示。

NSFOCUS

常见问题及处理方法

问题二：加固风险如何规避

使用模拟环境

可以对加固方案进行验证，证明此次加固方案对被加固的在线业务系统是没有损害。

系统备份

对整个系统进行完全备份，包括系统和数据。发生故障时，可以快速恢复。

冗余备份

系统的所有模块均可以进行冗余分布式配置，不会因为任一单一模块的问题而出现全局故障。

恢复

加固系统所采用的备份方式进行系统恢复，保证系统最短时间内恢复运行。

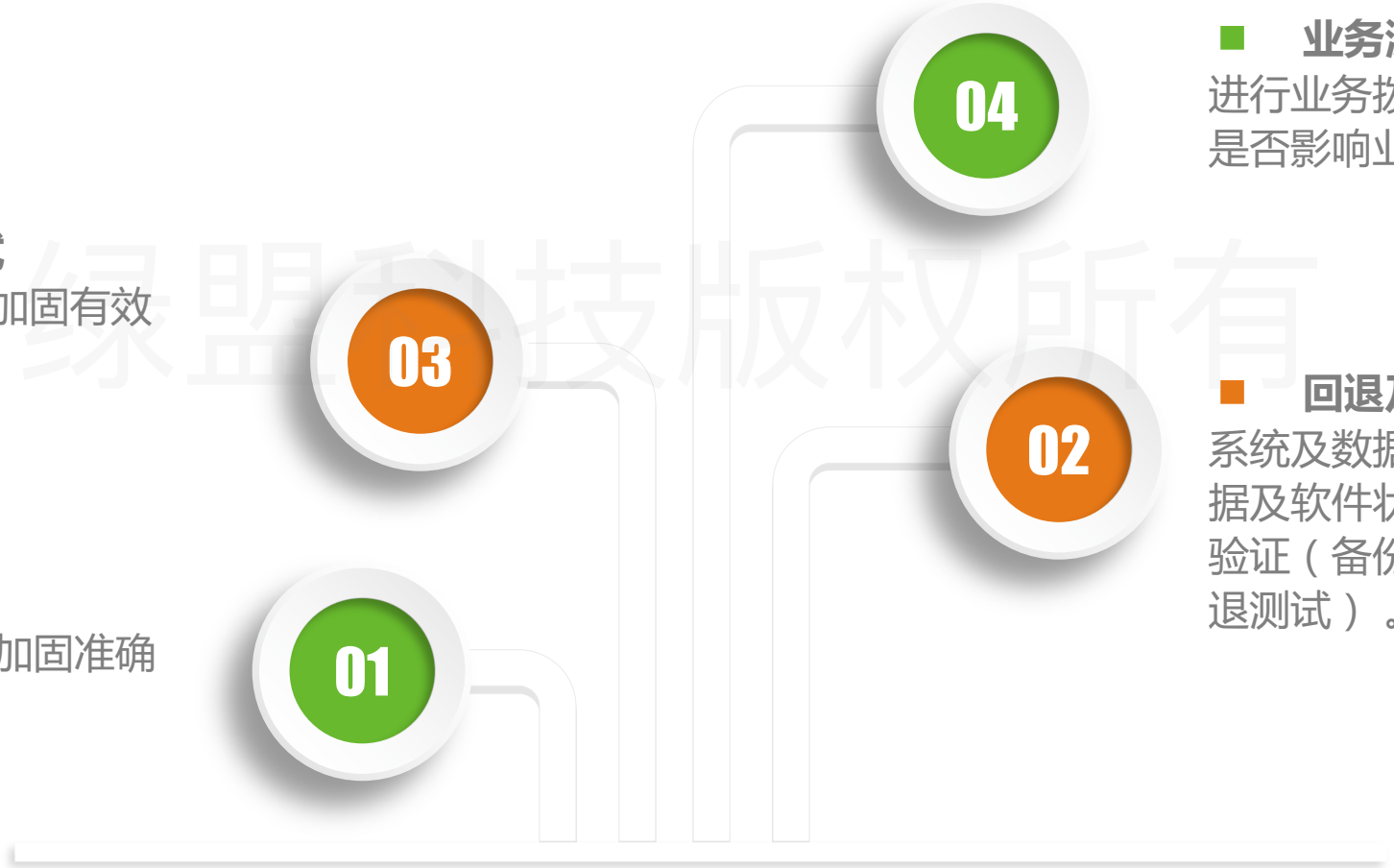
常见问题及处理方法

问题三：加固方案是否有效

- 明确加固的目标和范围，获取和熟悉系统的相关信息和服务信息（如：操作系统版本，数据库信息，中间件产品，类库，其它组件等）。
- 对该系统所承载的业务有一定的了解。包括系统内的主要核心流程，该系统与其他关联系统之间的接口与连接方式，该系统中断服务后对业务造成的影响等。明确每个加固项对系统造成的风险。
- 了解该系统变更管理策略，变更的审批流程与变更步骤。明确变更管理中各环节责任人以及其职责范围。获取变更管理的相关文档模板和工具。
- 会与客户进行方案的深层次沟通，完善加固实施手册。

常见问题及处理方法

安全加固测试：分为准备阶段的测试和实施阶段的测试。



- **业务测试**
  进行业务拨测，确认加固操作是否影响业务。

- **加固有效性测试**
  安全风险测试，确认加固有效性。

- **回退及可逆操作测试**
  系统及数据备份（备份业务数据及软件状态）以及回退操作验证（备份数据及软件状态回退测试）。

- **加固步骤测试**
  加固步骤测试，确认加固准确性。

常见问题及处理方法

问题四：运维中出现故障，是否为安全加固导致

02 同运维部门就安全加固过程中的人员分工、操作内容、时间等并进行备忘。

04 向运维技术人员表明态度，并做出行动，加固相关支持的将以持续性的姿态进行，不会在加固完结后终止。

01 同运维部门骨干和部门领导确认回退方案，认可回退方案的可靠性和可行性。

03 对相关运维技术人员进行培训，重点在于回退技术的反复演练。并让运维部门领导了解到此技术，在部门内进行强化。

谢谢！

NSFOCUS