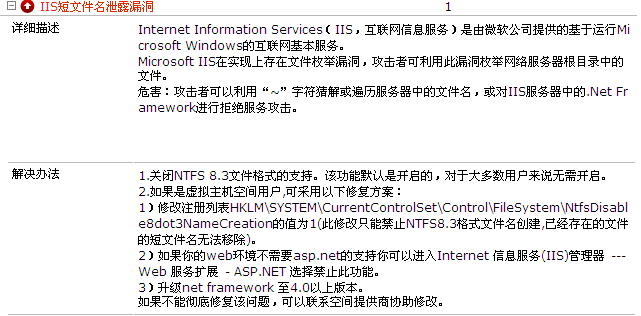
无线城市美食通——IIS短文件名漏洞

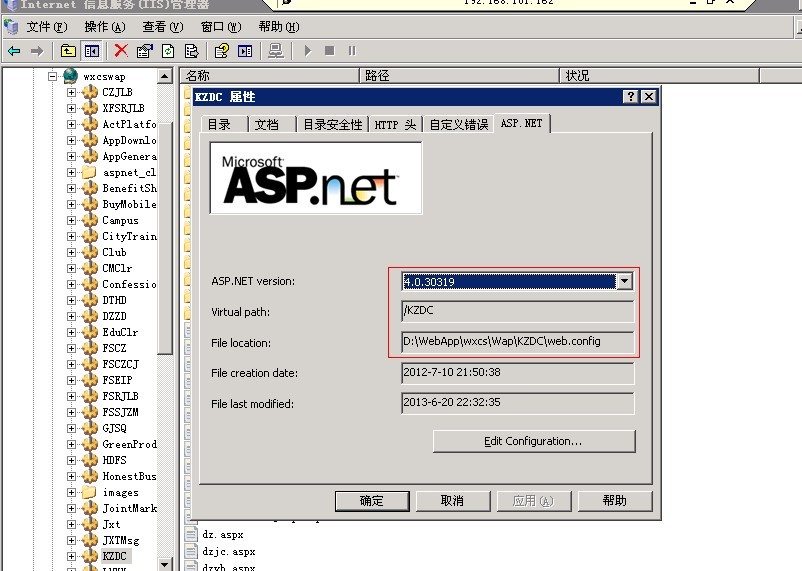
# 一、IIS短文件名泄露漏洞详细

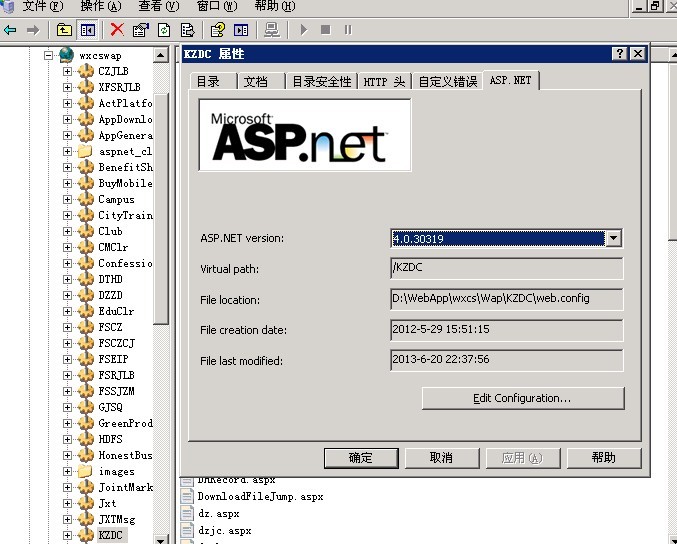


# 二、IIS短文件名修复方式

1）、升级net framework到4.0版本，修改注册表

升级net framework到4.0版本以后，扫描正式环境192.168.101.162端口7001\7002，漏洞依然存在，如下图





2）、关闭NTFS 8.3文件格式的支持，测试环境实现方式

关闭NTFS 8.3文件格式的支持以后，必须是新建的文件夹，在新建文件夹下从新配置IIS站点且net framework版本为4.0，漏洞不存在

测试环境操作步骤：

1. 在192.168.100.3服务器，新建d:\webapptest\wxcs\wap\KZDC，d:\webapptest\wxcs\web\KZDC美食通文件夹
2. TSM 恢复美食通站点文件到对应路径
3. 在服务器新建美食通WEP站点KZDC,端口号7005，站点路径指向新增的文件夹wap\KZDC
4. 在服务器新建美食通WEB站点KZDC,端口号7006，站点路径指向新增的文件夹web\KZDC

# 三、IIS短文件名解决方案建议

关闭NTFS 8.3文件格式的支持且升级，net framework版本为4.0，只是保障以后新建文件夹配置站点时候，可以解决此漏洞；对于已存在的文件夹和站点，漏洞依然存在。因此，如需要解决已存在的漏洞问题，需要删除现有所有文件夹和站点，需从新创建文件夹且在IIS从新配置站点。

测试环境操作步骤：

1. 关闭NTFS 8.3文件格式的支持且升级，net framework版本为4.0
2. 删除原有IIS漏洞站点和文件夹
3. 创建站点物理文件夹，TSM恢复站点数据
4. IIS上新建站点，指向新创建的物理文件夹

# IIS短文件名漏洞报告

1. 升级net framework版本为4.0报告（正式环境IP:192.168.101.162\163）

美食通wap\_2013-12-05\_14-06-23.zip

美食通商家界面-1\_2013-12-05\_13-10-59.zip

7002\_2013-12-05\_16-40-50.zip

2、关闭NTFS 8.3文件格式的支持且升级，net framework版本为4.0（测试环境IP:192.168.100.3）

扫描［192.168.100.37006］\_2013-12-09\_15-37-50.zip

扫描［192.168.100.37005]\_2013-12-09\_15-29-42.zip