（一）IIS

1、PUT 漏洞

2、短文件名猜解

3、远程代码执行

4、解析漏洞

参考：

<https://www.cnblogs.com/sunshineyan/p/8954532.html>

http://www.mchz.com.cn/cn/service/Safety-Lab/info\_26\_itemid\_2068.html

一.put漏洞

开启webdav 且允许写权限（两个限制）

工具检测 davtest -url “”

预防：

关闭webdav的组件，关闭写权限

1. 短文件

分析：<http://www.lijiejie.com/iis-win8-3-shortname-brute/>

扫描：

<https://github.com/lijiejie/IIS_shortname_Scanner/blob/master/iis_shortname_Scan.py>

预防（未测试）：

修复方法：修改注册列表HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation的值为1，重启服务器。此方法禁止NTFS8.3格式文件名创建

重新上传网站文件即可

1. 远程代码执行

iis6.0远程代码执行漏洞复现(CVE-2017-7269)，参考：<https://blog.csdn.net/darkhq/article/details/79127820>

use exploit/windows/iis/cve-2017-7269 （msf利用，要先加rb模块，参考：<https://blog.csdn.net/gp1531620582/article/details/80699670）>

预防：

打补丁

1. 解析漏洞

主要结合上传漏洞

个人以前的总结：

<http://www.youknowi.xin/2018/09/%e5%85%b8%e5%9e%8b%e6%bc%8f%e6%b4%9e%e5%bd%92%e7%ba%b3%e4%b9%8b%e4%b8%8a%e4%bc%a0%e6%bc%8f%e6%b4%9e%ef%bc%88%e8%bd%ac%e8%bd%bd%ef%bc%89/>

http://www.youknowi.xin/2018/10/%e6%96%87%e4%bb%b6%e4%b8%8a%e4%bc%a0%e7%9a%84%e5%a7%bf%e5%8a%bf/



预防：

微软不承认是漏洞，未找到方法，可在上传处预防

白名单+重命名