**2207.com系统技术检测报告**

系统属地： 厦门

系统名称： 2207.com

域名（或IP地址）： 2207.com

技术检测报告

经技术检测发现，你单位系统（域名或IP地址:2207.com:80存在安全漏洞1个，其中高风险漏洞1个，中风险漏洞0个，低风险漏洞0个，已验证漏洞1个。

**1.检测结果（检测结果包含但不限于以下漏洞）**

**1.1 高危风险漏洞**

**1.1.1 MS15-034 HTTP.sys远程代码执行**

http://2207.com/

**漏洞描述:**

目标存在HTTP.sys远程执行代码漏洞（CVE-2015-1635，MS15-034）。远程执行代码漏洞存在于 HTTP 协议堆栈 (HTTP.sys) 中，当 HTTP.sys 未正确分析经特殊设计的 HTTP 请求时会导致此漏洞。如果攻击者向受影响的 Windows 系统发送经特殊设计的的 HTTP 请求，此漏洞可能允许远程执行代码。

**1.2 中危风险漏洞**

**1.3 低危风险漏洞**

**2.验证结果**

仅对上述漏洞中威胁较高的漏洞进行验证，请你单位自行验证其他漏洞。

验证地址或请求：

验证截图

请你单位高度重视系统安全保障工作，对系统进行全面检测、整改，有关整改情况及时反馈同级公安机关网安部门。

附件：漏洞危害及整改建议

系统漏洞危害及整改建议

1. MS15-034 HTTP.sys远程代码执行

*漏洞危害:*

攻击者可以利用该漏洞在系统帐户的上下文中执行任意代码，可能导致目标服务器蓝屏死机。

*整改意见:*

1.安装补丁控制面--系统和安--更新--安装KB3042553号补丁。(重启生效)2.参考Microsoft 安全公告进行修复https://technet.microsoft.com/zh-cn/library/security/MS15-034