**威胁响应：Windows HTTP.sys远程代码执行漏洞跟踪进展**

2015.04.15夜，绿盟科技在官方微博发布了此漏洞通告，公告编号：Alert2015-04，CVE ID：CVE-2015-1635，受此漏洞影响的软件及系统包括：

Microsoft Windows Server 2012 R2

Microsoft Windows Server 2012

Microsoft Windows Server 2008 SP1

Microsoft Windows 8.1

Microsoft Windows 8

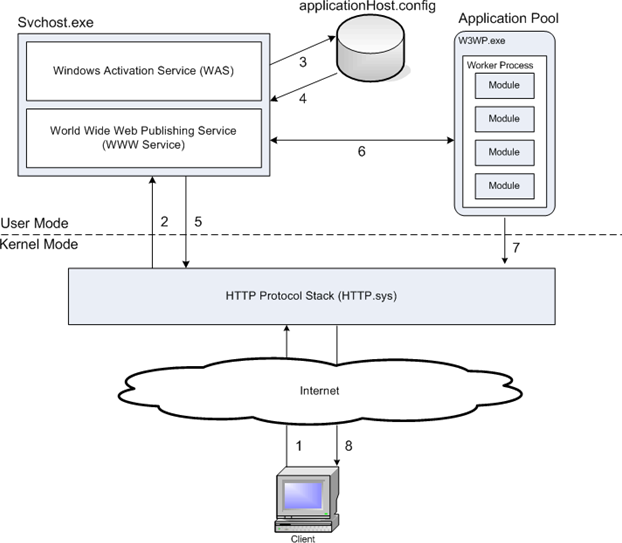
Microsoft Windows 7 SP1

**解决办法**

* **请所有使用如上系统的用户尽快升级补丁**
  + 厂商已在安全公告MS15-034中修复了此安全漏洞。我们建议用户开启自动更新服务以及时安装最新补丁，补丁可以通过Windows update在线获得。相关公告请见如下链接：  
    <http://technet.microsoft.com/security/bulletin/MS15-034>
  + **如果您的业务系统暂时还无法升级补丁，**那么可通过禁用IIS 内核缓存来临时缓解此漏洞的危险，虽然这可能会导致IIS性能下降，但总比出安全事故的好啊，具体的执行方法可以参考如下链接：  
    <https://technet.microsoft.com/zh-cn/library/cc731903(v=ws.10).aspx>
* **请所有使用绿盟科技产品的客户尽快升级产品规则**
  + 绿盟科技已在软件升级公告中提供规则升级包，NIPS、WAF、RSAS、WVSS、NF的用户请尽快升级最新规则，规则可以通过产品界面的在线升级进行。
  + **如果您的业务系统暂时还无法升级规则包**，那么可以在软件升级页面中，找到对应的产品，通过下载升级包，以离线方式进行升级。具体公告请参考如下链接：  
    <http://update.nsfocus.com/>

**http.sys的重要性解读**

Http.sys是Microsoft Windows处理HTTP请求的内核驱动程序。HTTP.sys会错误解析某些特殊构造的HTTP请求，导致远程代码执行漏洞。成功利用此漏洞后，攻击者可在System帐户上下文中执行任意代码。由于此漏洞存在于内核驱动程序中，攻击者也可以远程导致操作系统蓝屏。看看下图你就会了解到http.sys的重要性。



此次受影响的系统中，Windows 7、Windows 8、Windows Server 2008 R2 和 Windows Server 2012所带的HTTP.sys驱动均存在一个远程代码执行漏洞，远程攻击者可以通过IIS 7（或更高版本）服务将恶意的HTTP请求传递给HTTP.sys驱动，通过发送恶意的HTTP请求导致远程代码执行或操作系统蓝屏。这种利用方式相当容易，目前已经有可远程触发操作系统蓝屏的攻击代码流传。

**小贴士：**如何确定自己的电脑上IIS是否启用?

* Winkey+R打开运行对话框，输入services.msc回车，打开服务管理窗口，查看是否存在World Wide Web Publishing Service，如果服务状态是启用，表明IIS已经启用。

**威胁情报**

Threat intelligence 威胁情报无论对于解决传统安全或者APT攻击来说都是重要的手段之一，而随着0day漏洞频出，威胁情报的获取及响应都体现了防御能力的建设程度，而且这些能力建设需要不断的累积，从知识库到团队，从响应到分析到前瞻性预测，安全威胁情报市场已经逐步形成，这些情报将会以各种形式交付给企业和组织，成为其安全防御必不可少的一环。

威胁情报服务体系至少包含了威胁监测及响应、数据分析及整理、业务情报及交付、风险评估及咨询、安全托管及应用等各个方面，涉及研究、产品、服务、运营及营销的各个环节，绿盟科技威胁响应体系已经具备了这些要素，在不同的行业中向企业和组织持续服务，保障客户业务的顺畅运行。

**Security+报告**

另一方面，绿盟科技研究院也会长年跟踪分析这些威胁，将情报整理汇总并进行深入解读形成各种报告，大家平时看到的Security+系列就是这些报告的呈现，大家可以在绿盟科技官方网站、各类传统及社交媒体、售前售后服务、直邮刊物及邮件、市场活动及交流中获取它们，如果您还没有获取到这些报告，可以随时通过在微博、微信中搜索**绿盟科技**联系我们，欢迎您的垂询！