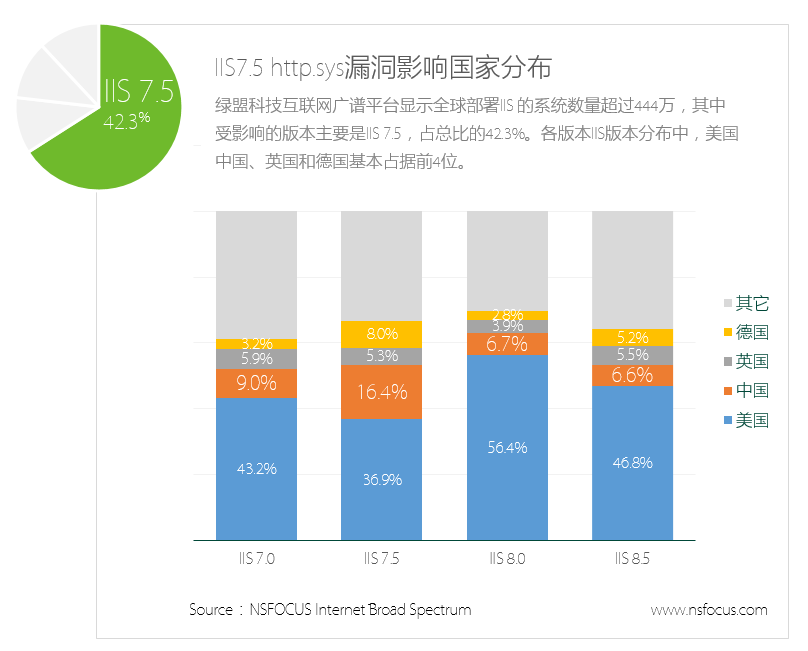
**深入解读：Windows HTTP.sys远程代码执行漏洞跟踪进展**

**摘要：（请媒体发布使用此小节内容）**

此次微软公告MS15-034 IIS7 http.sys漏洞，引来业界的关注，其震荡性不亚于Windows领域的心脏出血事件。绿盟科技威胁响应中心启动紧急响应机制，在4月15日、4月16日分别发布紧急通告及产品规则升级通告，请受影响的用户尽快升级厂商的补丁及绿盟科技产品规则包。

据绿盟科技互联网广谱平台数据显示，全球部署IIS的系统数量大概有444万余，从目前受影响的IIS各版本分布统计数据来看，其中IIS 7.5部署量最大，占比42.3%，也是本次漏洞追踪分析的重点。



经过绿盟科技研究院的深入分析，利用此漏洞的攻击大致会有两种形式：一种，攻击门槛比较低，很容易通过攻击导致服务器系统蓝屏；第二种，如果攻击者的水平比较高，就可以精确的控制内存，通过远程执行代码获得对系统的完全控制。尤其是面临高价值回报的攻击目标时，发生的几率就更高了，企业或组织的IT人员需要尽快考虑应对方案，避免在安全防御措施上线之前遭受攻击。

此次http.sys漏洞危害不可轻视，特别是一些大型的企业和组织，制定相关应对方案及执行措施需要一段时间，在此时间内建议按照如下步骤，以免在全面加固之前受到利用该漏洞的攻击，遭受不必要的损失。建议http.sys漏洞应对方案如下：

1. **尽快了解漏洞的相关信息，包括漏洞的影响范围和深度；**
2. **使用工具对业务系统进行安全的、全面的扫描，以便为方案制定提供依据；**
3. **邀请漏洞相关厂商及安全厂商一起，从业务稳定性、危害程度和范围及重要性等多个维度综合考虑，制定整改时间计划表和细化方案；**
4. **加固完成后，再次进行完整扫描、人工验证整改加固结果，以及分析业务系统日志，识别加固期间是否遭受攻击；**
5. **整体工作完成后，切记要进行总结和备案记录，如果后续有需求，可以追溯及备查。**

**正文：**

此次微软公告MS15-034 IIS7 http.sys漏洞，引来业界的关注，其震荡性不亚于Windows领域的心脏出血事件。绿盟科技威胁响应中心启动紧急响应机制，在4月15日、4月16日分别发布紧急通告及产品规则升级通告，受如下系统影响的用户还请尽快升级厂商的补丁及绿盟科技产品规则包。

Microsoft Windows Server 2012 R2

Microsoft Windows Server 2012

Microsoft Windows Server 2008 R2 SP1

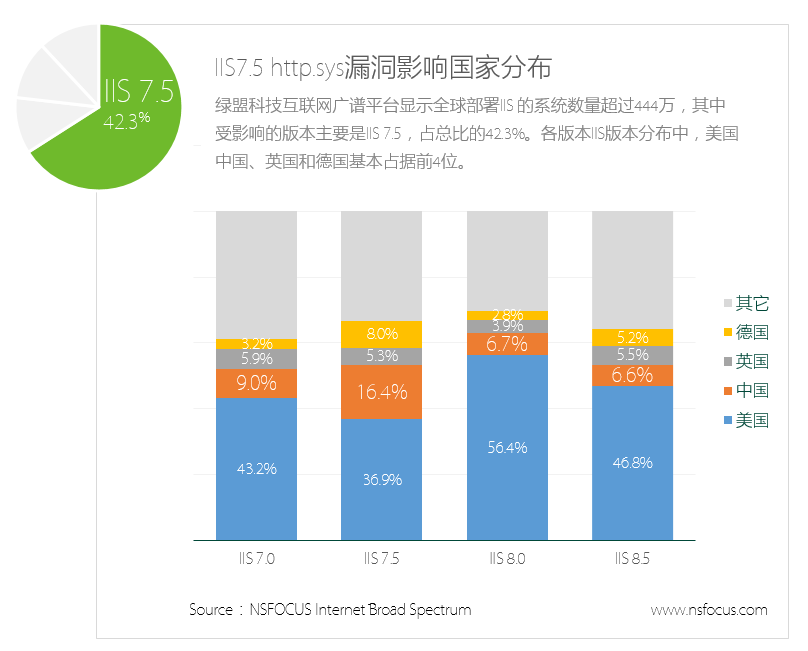
Microsoft Windows 8.1

Microsoft Windows 8

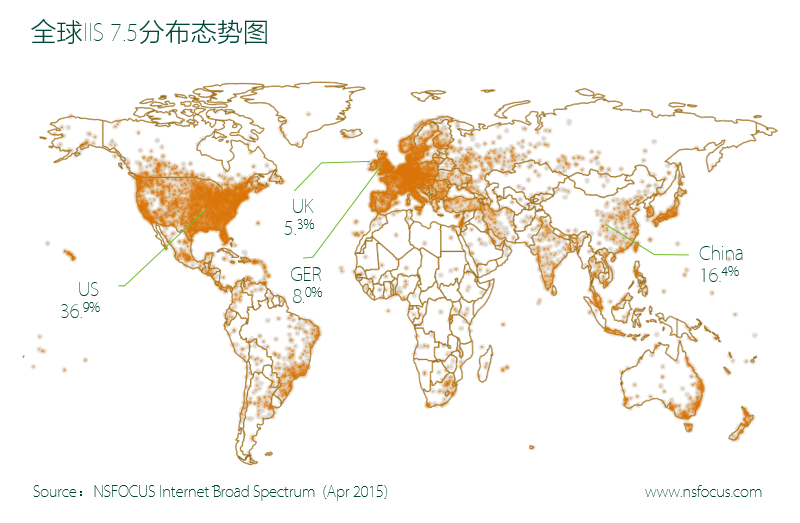
Microsoft Windows 7 SP1

**http.sys漏洞影响范围**

随着各方的深入分析，各地域受Windows HTTP.sys漏洞影响的情况正在逐渐浮出水面。昨天的通告信息中提到Http.sys是Microsoft Windows处理HTTP请求的内核驱动程序，据绿盟科技互联网广谱平台数据显示，全球部署IIS的系统数量大概有444万余，从目前受影响的IIS各版本分布统计数据来看，其中IIS 7.5部署量最大，占比42.3%，也是本次追踪分析的重点。



在如下全球IIS7.5分布态势图中，可以看到美洲、欧洲、亚洲等国家受影响比较严重，其中美国、中国、英国及德国为受影响的稠密区域。



**http.sys漏洞危害性分析**

很多大型企业或组织在应对http.sys漏洞的时候，往往需要采取谨慎的态度，对于应对措施需要，并且结合自身的业务情况及网络环境，定制行动计划，以避免对业务系统造成损害，这就需要深入了解此次漏洞的原理，才能给出合适的方案。未知攻焉知防！下面对此漏洞的原理进行分析，以便大家更好的理解和防御这一高危安全漏洞。

**1、漏洞触发**

根据Pastebin上披露的PoC（<http://pastebin.com/ypURDPc4>），很容易构造出能触发BSOD的PoC，比如以下请求：

GET /welcome.png HTTP/1.1

Host: PoC

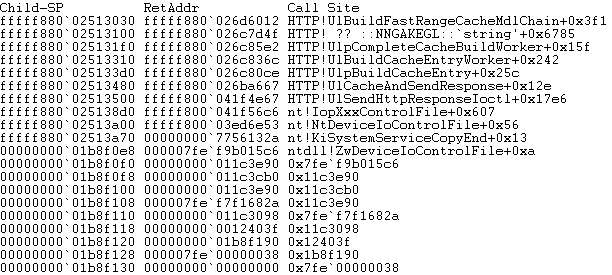
Range: bytes=12345-18446744073709551615

可以使安装有IIS 7.5的Windows 7 SP1系统BSOD。

**2、漏洞原理**

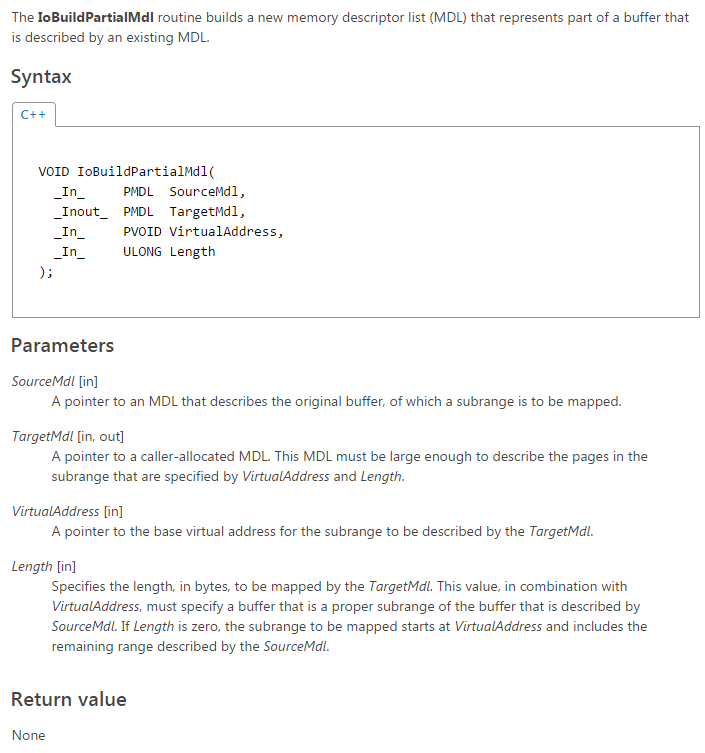
这里以Windows 7 SP1 X64系统上安装的IIS 7.5为例进行分析，其内核的版本为6.1.7601.18409，HTTP.sys的版本为6.1.7601.17514。

对BSOD崩溃的现场进行分析，发现是各种情况的内存错误，由此推测触发漏洞后可能造成了内存破坏。对HTTP.sys的处理流程进行分析、逐步排查，可以确定内存破坏发生在函数HTTP!UlBuildFastRangeCacheMdlChain中，调用栈如下：



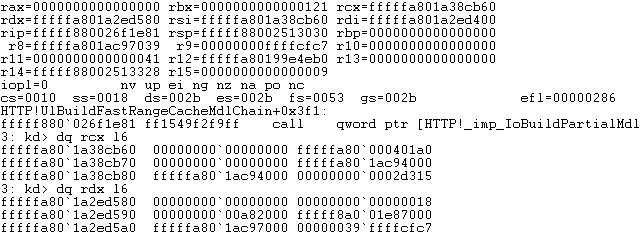
函数HTTP!UlBuildFastRangeCacheMdlChain用于生成响应报文的缓存MDL链，来描述HTTP响应的状态行、头部与消息体，链上的各MDL通过调用nt! IoBuildPartialMdl来生成。

MSDN中对nt! IoBuildPartialMdl的说明如下：



注意这里明确要求了由VirtualAddress与Length确定的区间必须是SourceMdl描述的缓冲区的一个自区间，正是对此要求的违反导致了此漏洞中的内存破坏。

第3次调用nt! IoBuildPartialMdl来生成消息体MDL时的参数如下：



SourceMdl = 0xfffffa801a38cb60

SourceMdl.VirtualAddress = 0xfffffa801ac94000

SourceMdl.ByteCount = 0x2d315

SourceMdl.ByteOffset = 0x0

TargetMdl = 0xfffffa801a2ed580

TargetMdl.VirtualAddress = 0xfffffa801ac97000

TargetMdl.ByteCount = 0xffffcfc7

TargetMdl.ByteOffset = 0x39

VirtualAddress = 0xfffffa801ac97039

Length = 0xffffcfc7

这里的Length是根据HTTP请求消息头部中的Range字段计算得到的，过程如下：

首先，在HTTP!UlpParseRange中对Range字段进行解析，得到RangeBegin、RangeEnd；

然后，计算RangeLength = RangeEnd - RangeBegin + 1；

最后，将RangeLength截断为32位得到Length。

以PoC中的Range: bytes=12345-18446744073709551615为例：

RangeBegin = 12345 = 0x3039

RangeEnd = 18446744073709551615 = 0xffffffffffffffff

RangeLength = 0xffffffffffffffff - 0x00003039 + 1 = 0xffffffffffffcfc7

Length = 0xffffcfc7

显然由于Length超长而导致违反了nt! IoBuildPartialMdl的要求，进而造成内存破坏。

**3、限制条件**

HTTP.sys中的一些校验措施可能在进入HTTP!UlBuildFastRangeCacheMdlChain函数前将RangeLength修改为合法值，从而不会触发漏洞。

例如，在Windows 7 SP1 X64系统的IIS 7.5中，函数HTTP!UlAdjustRangesToContentSize会对RangeLength进行检查，并在必要时进行调整，如下：

当RangeBegin >= ContentLength时，移除对应的数据；

当RangeLength== -1时，RangeLength= ContentLength – RangeBegin；

当RangeEnd + 1 >= ContentLength时，RangeLength= ContentLength – RangeBegin；

因此，要保持RangeLength不被修正而又能触发漏洞，必须要同时满足RangeEnd + 1 < ContentLength与RangeEnd > ContentLength，RangeEnd就只能为0xffffffffffffffff。

这样，RangeBegin就必须小于ContentLength，同时还不能为1（否则将使RangeLength = 0xffffffffffffffff – 1 + 1 = -1而导致RangeLength被修正）。

在其他版本的系统中可能会有更多的限制。

**4、代码执行**

从上述分析可以看出，触发此漏洞可越界写数据而造成内存破坏，理论上存在远程执行代码的可能性。但是越界所写数据的长度下限由ContentLength决定，通常会是一个较大的值而立即使系统崩溃。即使目标服务器上存在一些大的文件，可以用来越界写少量数据，所写数据内容与被覆盖目标也很难控制。因此，在实际环境中想要稳定的利用此漏洞来执行代码是非常困难的。

**与http.sys漏洞攻击赛跑**

通过前面的分析可以看到，利用此漏洞的攻击大致会有两种形式：1种难度比较低，很容易导致服务器系统蓝屏；2如果攻击者的水平比较高，就可以精确的控制内存，通过远程执行代码，进而获得对系统的完全控制。尤其是面临高价值回报的攻击目标时，发生的几率就更高了，企业或组织的IT人员需要尽快考虑应对方案，避免在安全防御措施上线之前遭受攻击。这至少应该包含如下环节：

* 首先，应该第一时间获取漏洞通告及相关信息，了解此次漏洞的影响范围及深度。
* 再者，需要将通告和解读与自身实际IT业务系统状况相结合，全面判断出影响范围和程度（这包括对自身业务及对其客户的影响程度），这个判断过程，需要数据作为准确方案制定的事实依据，建议用户使用安全可靠的漏洞扫描工具，升级最新发布的插件或规则库，对全网进行安全扫描，拿到第一手数据后以便作为决策依据；
* 再次，IT人员需要从业务稳定性、危害程度和范围及重要性等多个维度综合考虑，制定整改时间计划表，权重由高到低依次对局部网络及主机设备或某业务系统设备展开整改和加固工作（建议邀请漏洞相关厂商及安全厂商一同参与）。
  + 这个阶段需要安全厂商提供专业技术协助，比如漏洞加固咨询、验证加固是否成功；同时需要了解安全厂商的哪些设备已经发布或即将发布防护规则，升级后即可进行防护；
  + 如果还没有采用任何一款安全设备，就需要采取临时防护措施，包括采用漏洞相关厂商及安全厂商的相关方案，为整体加固争取时间，避免在未加固整改成功之前这个窗口时间遭到攻击并受到损失，这样的情况在相当多的0day事件中屡见不鲜；
  + 另外，还需要漏洞相关厂商与安全厂商通力协作，互相沟通漏洞原理和利用过程，进行较深层次的解读，才能够促进漏洞相关厂商的开发人员深入了解这个漏洞并根据其自身情况进行代码层面的整改；
* 然后，在加固阶段性或整体完成后，需要再次进行完整扫描和人工验证整改加固结果，在技术投入允许的条件下，建议您再次进行各方面日志分析，观察整改加固期间有没有成功的攻击到其系统造成其他损失；
* 最后，在整体响应工作完成后，进行总结和备案记录。

**IIS漏洞情况**

前车之鉴后事之师，IIS由于使用量较大，出现的问题不少，总是给人以不踏实的感觉。其实在2014年，微软IIS就出现了两个高危漏洞，其中第2个**且目前厂商还没有提供补丁或者升级程序，**我们建议使用这些IIS版本的用户随时关注厂商的主页以获取最新版本，并咨询绿盟科技的服务人员！

1. 2014-11-11，IIS安全功能绕过漏洞（MS14-076）（CVE-2014-4078）

描述：IIS 8.0/8.5版本的IP安全功能没有根据"IP Address and Domain Restrictions"列表正确处理进站Web请求，这可使远程攻击者通过HTTP请求，利用此漏洞绕过目标规则.

1. **2014-04-02，CGI CRLF注入漏洞（CVE-2011-5279）**

描述：Windows NT及Windows 2000上IIS 4.x及5.x版本的CGI实现中存在CRLF注入漏洞，这可使远程攻击者通过CGI请求中的\n字符（新行）构造畸形请求修改环境变量，从而进一步执行任意代码。

此外，IIS在其历史上也出过几次重大漏洞，绿盟科技研究院特别整理了这些信息，便于企业和组织的IT人员借鉴。**以下加粗字体，为目前厂商还没有提供补丁或者升级程序的漏洞，**请予以特别关注：

1. 2010-09-14 Microsoft IIS FastCGI请求头远程溢出漏洞（MS10-065）（CVE-2010-2730）

描述：对于启用了FastCGI功能的IIS服务器，远程攻击者可以通过提交特制的HTTP请求触发缓冲区溢出，导致执行任意代码。攻击者可以远程执行任意代码。

1. 2010-06-08 Microsoft IIS认证令牌处理远程代码执行漏洞（MS10-040）（CVE-2010-1256）

描述：IIS Web服务器在解析从客户端所接收到了认证信息时没有正确地分配内存，远程攻击者可以通过发送特制的认证报文导致以工作进程标识（WPI）的上下文中执行代码。必须启用了Extended Protection for Authentication功能才可以利用这个漏洞（默认为禁用）。攻击者可以远程执行任意代码。

1. 2009-10-13 Microsoft IIS FTPd服务NLST命令远程栈溢出漏洞（MS09-053）（CVE-2009-3023）

描述：攻击者可以导致拒绝服务或远程执行任意代码。Microsoft IIS内嵌的FTP服务器中存在栈溢出漏洞。如果远程攻击者对带有特制名称的目录发布了包含有通配符的FTP NLST（NAME LIST）命令的话，就可以触发这个溢出，导致拒绝服务或执行任意代码。仅在攻击者拥有写访问权限的情况下才可以创建带有特殊名称的目录。攻击者可以导致拒绝服务或远程执行任意代码。

1. **2009-09-15 Microsoft IIS脚本文件名错误解析漏洞**

描述：IIS在处理脚本文件名的解析时存在漏洞，当文件名为[YYY].asp;[ZZZ].jpg形式时，IIS会自动以asp格式来进行解析，而当文件名为[YYY].php;[ZZZ].jpg形式时，IIS会自动以php格式来进行解析（其中[YYY]与[ZZZ]为可变化字符串）。远程攻击者可以利用此漏洞突破Web应用对上传文件类型的限制，在服务器上执行任意脚本代码从而获取对服务器的控制。攻击者可以远程执行任意代码。

1. 2009-06-09 Microsoft IIS 5.0 WebDAV绕过认证漏洞（MS09-020）（CVE-2009-1122）

描述：IIS的WebDAV扩展没有正确解码特制请求的URL，导致WebDAV在处理该请求时应用不正确的配置。如果应用的配置允许匿名访问，则特制的请求可以绕过身份验证。请注意IIS在配置的匿名用户帐户的安全上下文中仍会处理该请求，因此此漏洞不能用于绕过NTFS ACL，文件系统ACL对匿名用户帐户强加的限制将仍然执行。攻击者可以绕过认证获得非授权访问。

1. 2009-06-09 Microsoft IIS WebDAV Unicode请求绕过认证漏洞（MS09-020）（CVE-2009-1535）

描述：IIS的WebDAV功能在解析URI并发送回数据时没有正确地处理Unicode令牌环，远程攻击者可以通过提交恶意HTTP GET请求绕过受口令保护的文件夹的认证，或在受口令保护的WebDAV目录中列出、上传或下载文件。攻击者可以绕过认证执行非授权操作。

1. 2008-02-12 Microsoft IIS ASP远程代码执行漏洞（MS08-006）（CVE-2008-0075）

描述：IIS处理ASP网页输入的方式存在远程代码执行漏洞，允许攻击者向网站的ASP页面传送恶意输入。成功利用这个漏洞的攻击者可以在IIS服务器上以WPI的权限（默认配置为网络服务帐号权限）执行任意操作。攻击者可以远程执行任意代码。

**请持续关注相关漏洞信息**

绿盟科技研究院会长年跟踪分析这些漏洞，并将整理后的结果发送给您，便于您持续关注漏洞的发展态势，为企业及组织的安全方案提供数据及信息支撑，如果您对我们提供的内容有任何疑问，或者需要了解更多的信息，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！