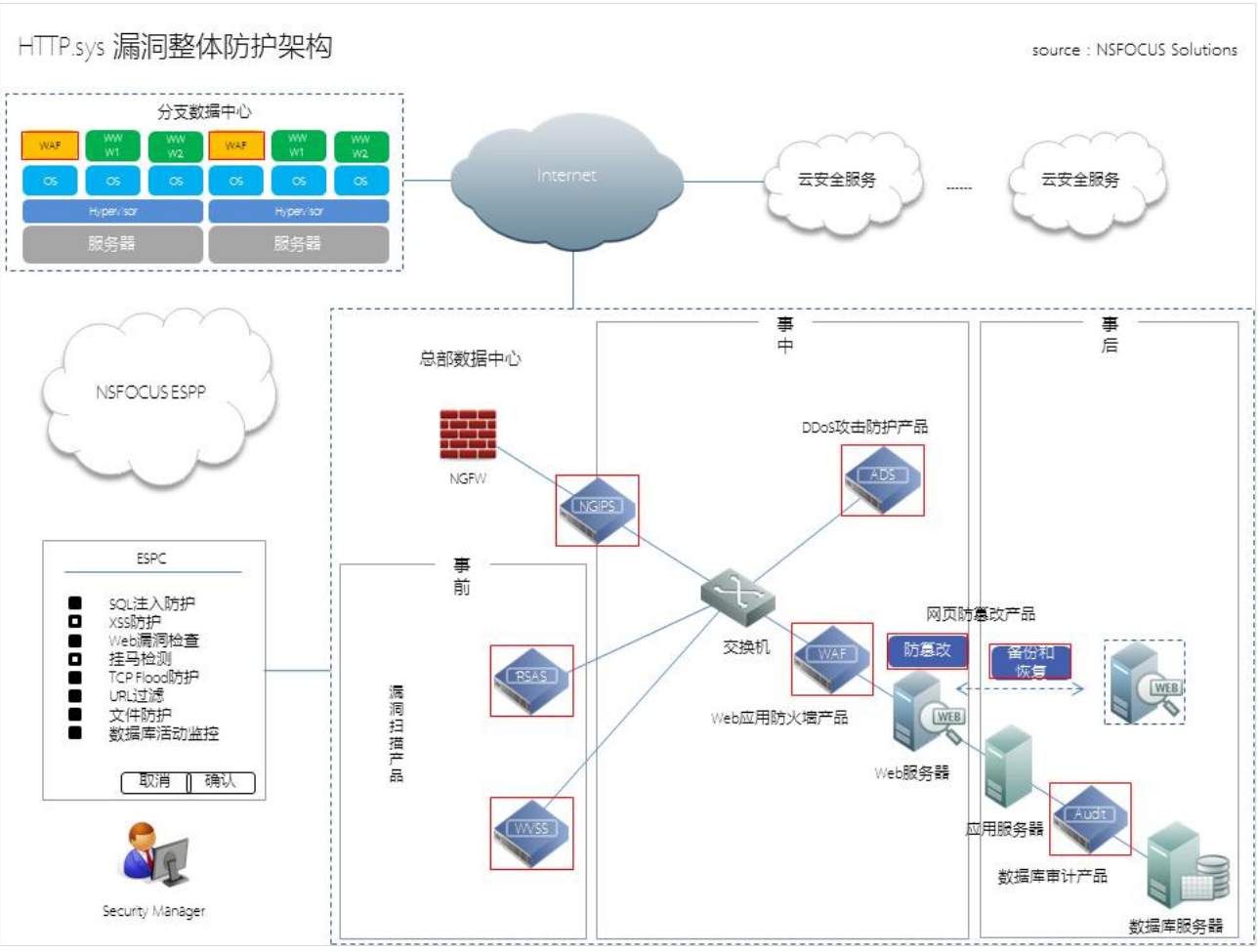
IIS 7 HTTP.sys 漏洞防护方案



Content

http.sys 漏洞回顾 3

受影响区域分布 3

http.sys 漏洞分析 5

http.sys 蓝屏 5

http.sys 漏洞利用 5

http.sys 漏洞检测 5

http.sys 漏洞云端检测 5

http.sys 漏洞产品端检测 6

http.sys 漏洞离线检测 7

http.sys 漏洞防护 10

漏洞加固 10

产品防护 10

业务安全加固 11

威胁情报 12

关于绿盟科技 12

执行摘要

4 月 14 日，微软公告 MS15-034/CVE-2015-1635 IIS7 http.sys 漏洞，绿盟科技威胁响应中心随即启动应急机制， 应急响应工作随即启动。

1. 15 日夜，发布高危漏洞紧急通告①②，支撑信息来自漏洞的利用机制分析及 POC 验证工作，第一时间告知客户关注；
2. 16 日，发布产品规则升级通告，绿盟科技 NIPS、WAF、RSAS、WVSS、NF 等产品升级相继就绪，客户通过在线及离线升级的方法，即可进行防护；
3. 17 日，发布漏洞深入分析，大型企业及组织客户可以通过这些信息定制自己的防御方案。在线漏洞检测引擎就绪。
4. 21 日，我们回顾 http.sys 漏洞的信息要点，从 http.sys 漏洞防护的角度进行总结，为大家制定防御方案提供补充信息。

如果您需要了解更多信息，请联系：

绿盟科技威胁响应中心微博

http://weibo.com/threatresponse

绿盟科技微博

http://weibo.com/nsfocus

绿盟科技微信号

搜索公众号 绿盟科技

① http://www.nsfocus.net/vulndb/29720

① http://weibo.com/1686253095/CdraocnA0

http.sys 漏洞回顾

4 月 14 日，微软公告了 https.sys 漏洞，即 Windows http.sys 远程代码执行高危漏洞（MS15-034），CVE 编号 CVE-2015-1635. 此漏洞由于具备如下的 4 个特点，一经发布，迅速引发攻击者的关注，在漏洞发布的第 2 天，Twitter 及新浪微博上出现大量漏洞信息，一些匿名的 POC 及可远程触发操作系统蓝屏的攻击代码开始流传。

1. Http.sys 是处理 HTTP 请求的内核驱动程序，处于咽喉要道，一旦被利用后患无穷；
2. 该漏洞很容构造特定的 http 请求，导致攻击目标蓝屏，这形式常见于不正当商业竞争；
3. 一旦被利用成功，可以获得很高的系统权限，可在 System 帐户上下文中执行任意代码；
4. IIS 在全球的部署总量超过 444 万[①]，但常常是未经加固或防护力量薄弱

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 R2 SP1

Microsoft Windows 8.1

Microsoft Windows 8

Microsoft Windows 7 SP1

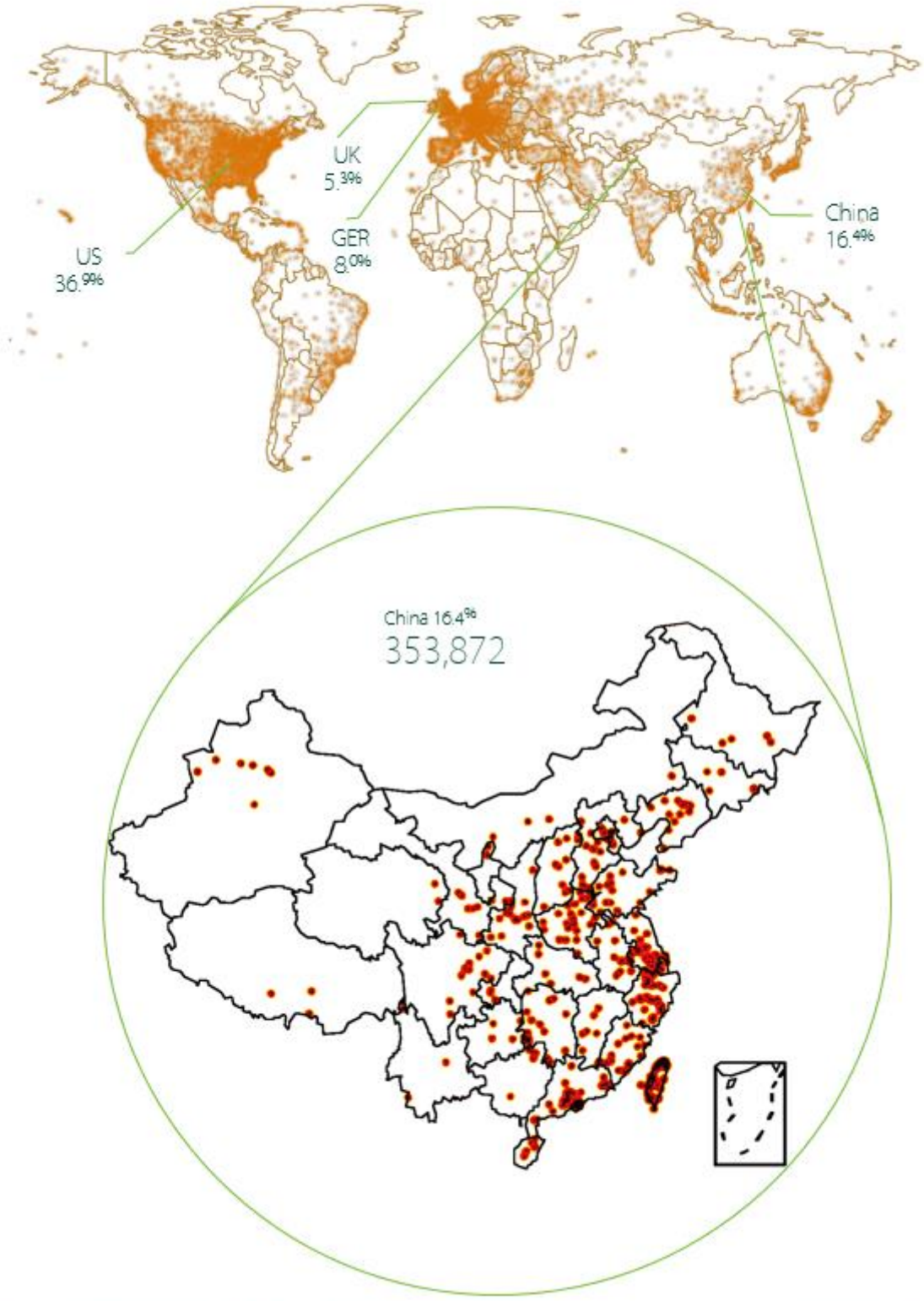
绿盟科技与漏洞相关厂商长年保持密切合作关系。绿盟科技威胁响应中心在获知相关信息后，随即启动应急机制，相关工作随即启动。

受影响区域分布

截止 2015 年 4 月 15 日，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。以占比最大的 IIS 7.5（42.3%）为例，美国、中国、英国及德国为受影响的稠密区域，其中中国占比 16.4%，II7.5 的部署量超过 35 万，这也是此次漏洞如此受到关注的原因之一。

① http://www.nsfocus.com.cn/news/201504/911.html

IIS 7.5分布态势图



Source: NSFOCUS Internet Broad Spectrum (Apr 2015)

www.nsfocus.com

http.sys 漏洞分析

2015 年 4 月 15 日夜，绿盟科技威胁响应中心在获取 http.sys 漏洞影响范围数据的同时，也在迅速展开漏洞的分析工作，通过重现漏洞的攻击过程，分析其工作原理，得以清晰识别及检测该漏洞方法，在准确定义其威胁定级后，随即向我们的客户发出高危漏洞紧急通告。

http.sys 蓝屏

根据 Pastebin 上披露的 PoC[①]，很容易构造出能触发蓝屏（BSOD）的 PoC，比如以下请求：

```
1  GET /welcome.png HTTP/1.1
2  Host: PoC
3  Range: bytes=12345-18446744073709551615
```

可以使安装有 IIS 7.5 的 Windows 7 SP1 系统 BSOD。

http.sys 漏洞利用

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，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[②]。

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，但攻击者要想利用此漏洞使攻击目标蓝屏，是非常简单的事情！

正是考虑到蓝屏的因素，绿盟科技威胁响应中心在对外公布漏洞检测方法的时候尤为谨慎，避免给使用这些检测方法的用户造成不必要的二次伤害，经过反复验证安全可靠之后，才将检测方法投入云端检测系统。

http.sys 漏洞检测

面对如此严峻的形式，分析人员迅速将经过安全验证后的检测方法向云端、产品端及服务端传递，并建议用户尽快对其业务环境进行一次全面的漏洞检测，以便可以尽快拿到第一手数据，为后续制定漏洞防护方案及执行措施提供数据支撑及决策依据。http.sys 漏洞的检测方式可以使用三种方式，云端、产品端及脚本工具。

http.sys 漏洞云端检测

4 月 17 日晚 20:00，绿盟科技客户自助门户系统 Portal 发布 http.sys 漏洞检测引擎，为 Windows HTTP.sys 远程代码执行漏洞(CVE-2015-1635)应急扫描支持，截止至 4 月 19 日凌晨 3:00，已有 348 家客户，共提交并扫描域名数量 2086 个，其中 9 家客户

---

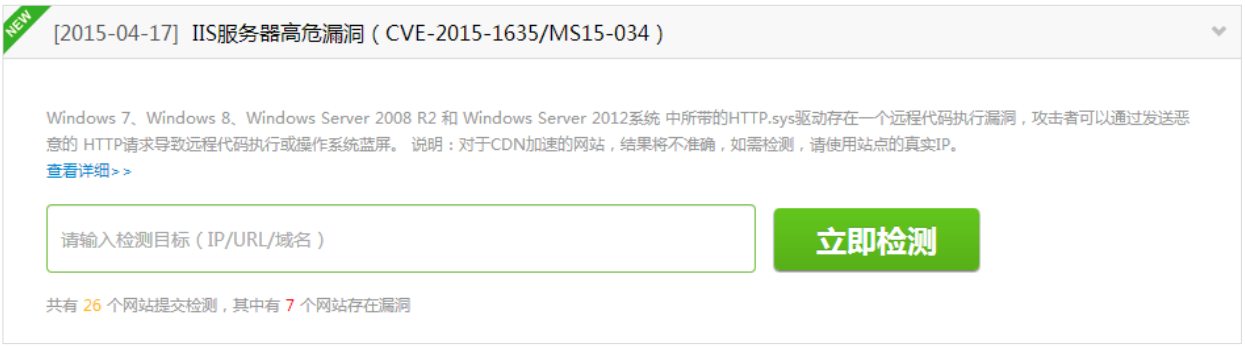
① http://pastebin.com/ypURDPc4

② NSFOCUS, 深入解读：Windows HTTP.sys 远程代码执行漏洞跟踪进展

存在 Windows HTTP.sys 远程代码执行漏洞，响应团队随即通知客户。同时绿盟科技漏洞扫描产品 RSAS、AAS 已在第一时间发布了检测插件升级包，随后 NF、IDS、IPS 也在 1 天内发布了产品规则升级包。

客户	数量	域名	数量
扫描客户	348	扫描域名	2086
存在 IIS 漏洞客户	9	存在 IIS 漏洞域名	10
不存在 IIS 漏洞客户	339	不存在 IIS 漏洞域名	1541

现在您随时可以使用这个自助系统，对业务环境进行扫描，以便确认是否存在该漏洞，扫描请点击：https://portal.nsfocus.com/vulnerability/list/



漏洞确认　　当扫描结果信息中出现信息"您的检测目标存在此漏洞"，即可确认当前业务环境中存在该漏洞，建议您尽快制定防护计划，以避免系统在获得加固前遭受攻击。

http.sys 漏洞产品端检测

4 月 16 日中午，绿盟科技各产品针对 http.sys 的规则升级包及插件升级包全部就绪，并在官方发布产品升级通告，同时向服务人员发送相关信息。这里将主要产品升级版本信息摘录如下，请广大用户尽快查看所使用产品的版本的信息，更多详细信息请查询：http://update.nsfocus.com/

http.sys 漏洞防护规则升级包

产品	版本号	升级时间	
NF 6.0.1	6.0.1.496	2015/4/16	12:00:00
NF 6.0.0	5.6.7.496	2015/4/16	12:00:00
IDS 5.6.9	5.6.9.12244	2015/4/16	13:00:00
IDS 5.6.8	5.6.8.496	2015/4/16	11:00:00
IDS 5.6.7	5.6.7.496	2015/4/16	11:00:00
IDS 5.6.6	5.6.0.422	2015/4/16	11:00:00
IPS 5.6.9	5.6.9.12244	2015/4/16	11:00:00
IPS 5.6.8	5.6.8.496	2015/4/16	11:00:00
IPS 5.6.7	5.6.7.496	2015/4/16	11:00:00
IPS 5.6.6	5.6.0.422	2015/4/16	11:00:00
WAF 6.0.4	6.0.4.1.30345	2015/4/16	11:00:00

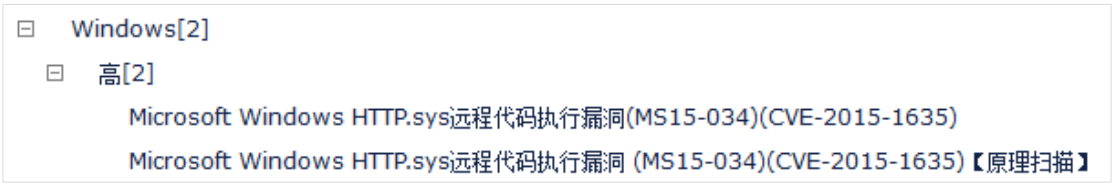
http.sys 漏洞防护插件升级包

产品	版本号	升级时间	
RSAS 6.0	V6.0R02F00.0108	2015/4/16	18:00:00
RSAS 5.0	051347	2015/4/16	19:00:00
RSAS-AAS 5.0	051130	2015/4/17	15:00:00
WVSS 6.0	V6.0R02F00.28	2015/4/16	18:00:00

如果您的业务环境中已经部署了相关漏洞扫描系统，请将漏洞扫描系统升级到最新版本后，尽快开始对业务系统进行扫描，尤其是受此次 http.sys 漏洞影响的业务系统平台进行一次漏洞扫描。这里以绿盟远程安全评估系统（NSFOCUS Remote Security Assessment System ，简称：NSFOCUS RSAS）为例，当您部署该产品后，请先对产品进行升级：

- RSAS v6 系列产品升级到系统插件版本 V6.0R02F00.0108；
- RSAS v5 系列产品升级到系统版本为 051347；
- AAS 系列产品升级到系统版本为 051130

漏洞确认　　如果您的漏洞扫描结果包含下图漏洞，特别是包含带有"【原理扫描】"字样的漏洞时，即可确认当前环境中存在该漏洞，建议您尽快制定防护计划，以避免系统在获得加固前遭受攻击。



http.sys 漏洞离线检测

如果您还没有部署漏洞扫描产品，又或者您的业务系统目前还不适合进行如上检测方式，还可以采用离线检测的方式，即采用 http.sys POC 验证。这里提供两种形式，包括 Python 脚本及 curl 工具。

> 小贴士：
>
> 这里提醒大家，近期受此漏洞影响，大量漏洞检测脚本及工具频出，如果您需要获取这些检测工具，需要从可靠途径获取，避免被植入恶意代码，以免前门拒狼后门进虎！

使用 python 脚本检测　将下列代码写入.py 文件执行即可。

```
'''
此脚本仅适用于检测 IIS 服务器是否存在 Http.sys 处理 Range 整数溢出漏洞，不适用于攻击使用。
'''
import socket
import random

ipAddr = ""        #添加目标 ip
hexAllFfff = "18446744073709551615"

req1 = "GET / HTTP/1.0\r\n\r\n"
req = "GET / HTTP/1.1\r\nHost: stuff\r\nRange: bytes=0-" + hexAllFfff + "\r\n\r\n"        #主要测试代码

print "[*] Audit Started"
client_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
client_socket.connect((ipAddr, 80))                    #如果 web 服务器开启非 80 端口，可在此处修改为正确端口
client_socket.send(req1)
boringResp = client_socket.recv(1024)
if "Microsoft" not in boringResp:                    #检测当前 web 服务是否为 IIS web 服务器
                print "[*] Not IIS"
                exit(0)
client_socket.close()
client_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
client_socket.connect((ipAddr, 80))
client_socket.send(req)
goodResp = client_socket.recv(1024)
if "Requested Range Not Satisfiable" in goodResp:                #通过查看服务器返回判断是否存在该漏洞，根据打印出的结果判断：
                                                                #Looks VULN 为存在该漏洞，Looks Patched 为已打补丁，其他情况会返回 Unexpected response
                print "[!!] Looks VULN"
elif " The request has an invalid header name" in goodResp:
                print "[*] Looks Patched"
else:
                print "[*] Unexpected response, cannot discern patch status"
```

使用 curl 工具检测

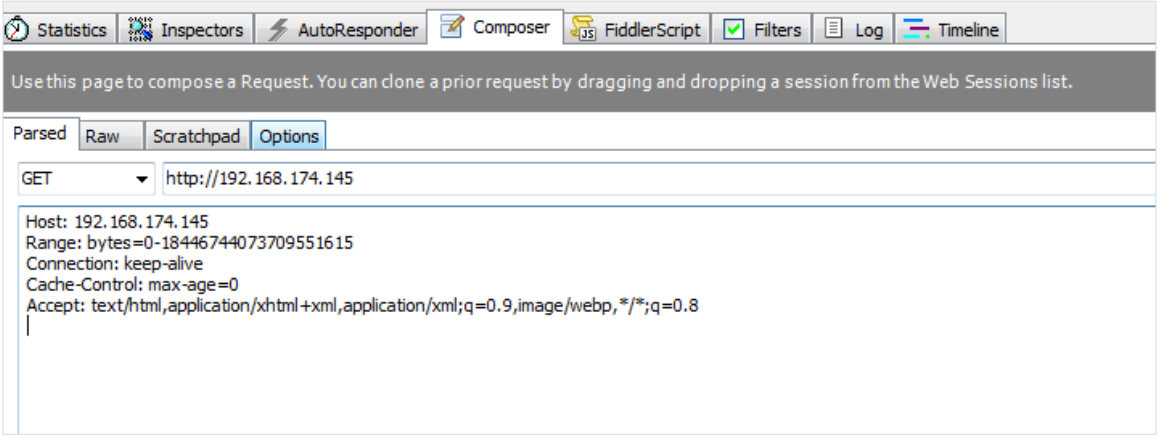
```
$curl -v 192.168.174.140 -H "Host: irrelevant" -H "Range: bytes=0-18446744073709551615"
```

漏洞确认　　存在此漏洞截图，如服务器返回 Requested Range Not Satisfiable，则说明存在此漏洞。建议您尽快制定防护计划，以避免系统在获得加固前遭受攻击。

```
[redacted]>curl -v 192.168.174.145 -H "Host: irrelevant" -H "
Range: bytes=0-18446744073709551615"
* About to connect() to 192.168.174.145 port 80 (#0)
*   Trying 192.168.174.145... connected
* Connected to 192.168.174.145 (192.168.174.145) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.19.3 (i386-pc-win32) libcurl/7.19.3 zlib/1.2.3
> Accept: */*
> Host: irrelevant
> Range: bytes=0-18446744073709551615
>
< HTTP/1.1 416 Requested Range Not Satisfiable
< Content-Type: text/html
< Last-Modified: Sat, 29 Sep 2012 02:55:06 GMT
< Accept-Ranges: bytes
< ETag: "609ddfd4ed9dcd1:0"
< Server: Microsoft-IIS/8.0
< X-Powered-By: ASP.NET
< Date: Fri, 17 Apr 2015 10:23:24 GMT
< Content-Length: 362
< Content-Range: bytes */1398
<
* Connection #0 to host 192.168.174.145 left intact
* Closing connection #0
```

使用发包工具构造 http 请求包检测　　以 fiddler 工具为例，构造如下图的请求包：

```
GET http://192.168.174.145/ HTTP/1.1
Host: 192.168.174.145
Range: bytes=0-18446744073709551615
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
```



漏洞确认　　如果收到服务器返回包如下，则说明存在此漏洞。建议您尽快制定防护计划，以避免系统在获得加固前遭受攻击。

http.sys 漏洞防护

经过上面的漏洞检测步骤后，如果确认您的业务环境中存在 http.sys 漏洞，那么就需要尽快制定并启动加固方案，这些加固从漏洞补丁开始，到产品防护，到整体防护，逐步推进。

漏洞加固

使用 IIS 的用户，可以通过 Windows Update 的方式获得对应的 KB3042553 热修补补丁，建议用户开启自动更新服务以及时安装最新补丁，相关公告请见：

http.sys 漏洞补丁公告：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，但需要注意这可能会导致 IIS 性能下降，具体的执行方法可以参考：

http.sys 漏洞缓解方案：https://technet.microsoft.com/zh-cn/library/cc731903(v=ws.10).aspx

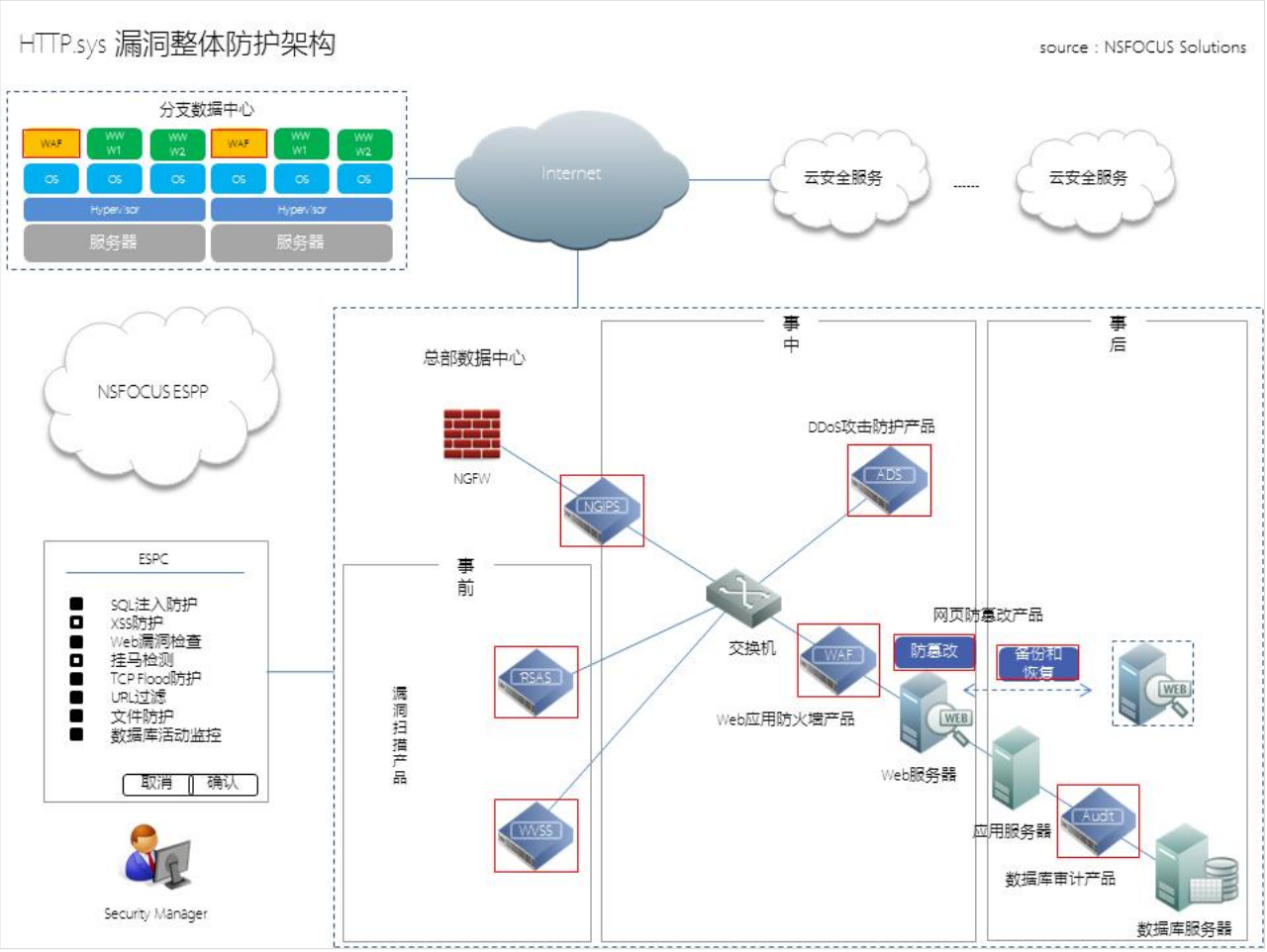
IIS 加固

虽然 IIS7 中 http.sys 已经独立出来成为系统级驱动程序，但以史为鉴，建议用户在安装补丁的同时也需要考虑 IIS 加固事项，具体的最佳实践请参考：

IIS7 加固方案： https://technet.microsoft.com/zh-cn/library/cc731278(WS.10).aspx

产品防护

如同木桶效应一般，业务环境的加固只是依赖于漏洞加固是不够的，整体安全等级的提升以及应对未来的攻击，安全产品是必不可少的一环，将 Web 系统置于 DMZ 区域并加以多产品的整体防护，是我们推荐的做法。在如下部署环境中，以绿盟 Web 应用防火墙（Web Application Firewall，简称 WAF）为例，对业务系统部署 WAF 能够从客户资产的视角，实施多种基于规则的检测，并实施多层次的安全机制，随时与云端服务协作，生成相应的 Web 安全解决方案，从而有效应对漏洞防护任务。



请所有使用绿盟产品的用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，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。 相关信息请访问：

- 安全产品介绍：http://www.nsfocus.com.cn/1_solution/1_2_1.html
- 产品升级公告：http://update.nsfocus.com/

业务安全加固

在一些大型的企业或组织中，http.sys 漏洞的防护或许并不能快速执行，其原因在于：1 需要考虑业务系统的可用性；2 需要考虑整体实施方案制定；3 需要尽可能降低加固动作对业务环境的二次伤害。这就需要企业自身、漏洞相关厂商、安全厂商一起协作才能形成快速、安全、有效的行动方案，避免业务系统在获得安全加固之前遭受攻击。在此次应急响应过程中，绿盟科技的服务人员向客户建议行动方案应该且至少包含如下环节：

- 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。

威胁情报

从此次 http.sys 漏洞情况可以看到，无论漏洞原理怎样，无论漏洞防护方案如何实施，关键在于尽可能快的了解到漏洞信息及相关的情报，以便尽可能快的启动应急响应机制。这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，威胁情报的获取及响应都体现了防御能力的建设程度，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，绿盟科技通过研究、云端、产品、服务等立体的应急响应体系，向企业和组织及时提供威胁情报并持续进行后续服务，保障客户业务的顺畅运行。

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！

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。