glibc CVE-2015-7547

# 漏洞原理

glibc getaddrinfo溢出漏洞。经研究发现，所有Debian、Red Hat以及更多其它Linux发行版，只要glibc版本大于2.9就会受到该溢出漏洞影响。攻击者可以通过该漏洞直接批量获取大量主机权限，漏洞的成因在于DNS Server Response返回过量的(2048 ) 字节, 导致接下来的response 触发栈溢出

# 这里写图片描述预备知识-DNS

## DNS头部

**标识ID**： 请求客户端设置的16位标示，服务器给出应答的时候会带相同的标示字段回来，这样请求客户端就可以区分不同的请求应答了。

**标志**：这里写图片描述

QR 1个比特位用来区分是请求（0）还是应答（1）。

OPCODE 4个比特位用来设置查询的种类，应答的时候会带相同值，可用的值如下：

* 0 标准查询 (QUERY)
* 1 反向查询 (IQUERY)
* 2 服务器状态查询 (STATUS)
* 3-15 保留值，暂时未使用

**AA 授权应答(Authoritative Answer)** - 这个比特位在应答的时候才有意义，指出给出应答的服务器是查询域名的授权解析服务器。

注意因为别名的存在，应答可能存在多个主域名，这个AA位对应请求名，或者应答中的第一个主域名。

**TC 截断(TrunCation)** - 用来指出报文比允许的长度还要长，导致被截断。

**RD 期望递归(Recursion Desired)** - 这个比特位被请求设置，应答的时候使用的相同的值返回。如果设置了RD，就建议域名服务器进行递归解析，递归查询的支持是可选的。

**RA 支持递归(Recursion Available)** - 这个比特位在应答中设置或取消，用来代表服务器是否支持递归查询。

**Z 保留值**，暂时未使用。在所有的请求和应答报文中必须置为0。

**RCODE 应答码(Response code)** - 这4个比特位在应答报文中设置，代表的含义如下：

* 0 没有错误。
* 1 报文格式错误(Format error) - 服务器不能理解请求的报文。
* 2 服务器失败(Server failure) - 因为服务器的原因导致没办法处理这个请求。
* 3 名字错误(Name Error) - 只有对授权域名解析服务器有意义，指出解析的域名不存在。
* 4 没有实现(Not Implemented) - 域名服务器不支持查询类型。
* 5 拒绝(Refused) - 服务器由于设置的策略拒绝给出应答。比如，服务器不希望对某些请求者给出应答，或者服务器不希望进行某些操作（比如区域传送zone transfer）。
* 6-15 保留值，暂时未使用。

**问题数QDCOUNT** 无符号16位整数表示报文请求段中的问题记录数。

**资源记录数ANCOUNT** 无符号16位整数表示报文回答段中的回答记录数。

**授权资源记录数NSCOUNT** 无符号16位整数表示报文授权段中的授权记录数。

**额外资源记录数ARCOUNT** 无符号16位整数表示报文附加段中的附加记录数。

## DNS查询问题

这里写图片描述32bit

**查询名QNAME** 要查找的名字，是一个或多个标识符的序列。每个标识符以首字节的计数值来说明随后标识符的字节长度，每个名字以最后字节为0结束，长度为0的标识符是根标识符。单个标识符最大长度为63字节。

**查询类型QTYPE** 每个问题有一个查询类型。2个字节(1-255)表示查询类型，取值可以为任何可用的类型值，以及通配码来表示所有的资源记录。

|  |  |  |
| --- | --- | --- |
| 名字 | 数值 | 描述 |
| A | 1 | 期望获得查询名的IP地址。 |
| NS | 2 | 一个授权的域名服务器。 |
| CNAME | 5 | 规范名称。 |
| PTR | 12 | 指针记录。 |
| HINFO | 13 | 主机信息。 |
| MX | 15 | 邮件交换记录。 |
| AXFR | 252 | 对区域转换的请求。 |
| ANY | 255 | 对所有记录的请求。(超集) |

**查询类：**

IN （1） 指互联网地址。

CS 2 the CSNET class (Obsolete - used only for examples in some obsolete RFCs)

CH 3 the CHAOS class

HS 4 Hesiod [Dyer 87]

查询类是类的一个超集

\* 255 any class

## 应答报文格式（回答\授权\额外信息）



**域名NAME** 资源记录包含的域名((len+data)\*+0x00)

**类型TYPE** 2个字节表示资源记录的类型，指出RDATA数据的含义

|  |  |  |
| --- | --- | --- |
| **值** | 协议类型 | 描述 |
| 1 | A | IPv4地址 |
| 2 | NS | 名字服务器 |
| 5 | CNAME | 规范名称定义主机的正式名字的别名 |
| 6 | SOA | 开始授权标记一个区的开始 |
| 11 | WKS | 熟知服务定义主机提供的网络服务 |
| 12 | PTR | 指针把IP地址转化为域名 |
| 13 | HINFO | 主机信息给出主机使用的硬件和操作系统的表述 |
| 15 | MX | 邮件交换把邮件改变路由送到邮件服务器 |
| 28 | AAAA | IPv6地址 |
| 252 | AXFR | 传送整个区的请求 |
| 255 | ANY | 对所有记录的请求 |

**类CLASS** 2个字节表示RDATA的类,一般为0x01

**生存时间TTL** 4字节无符号整数表示资源记录可以缓存的时间。0代表只能被传输，但是不能被缓存。

**资源数据长度RDLENGTH** 2个字节无符号整数表示RDATA的长度

**资源数据RDATA** 不定长字符串来表示记录，格式根TYPE和CLASS有关。比如，TYPE是A，CLASS 是 IN，那么RDATA就是一个4个字节的ARPA网络地址。

<https://www.nslookuptool.com/chs/>