**http 拒绝服务**

**1 详细描述**

缓慢的http拒绝服务攻击是一种专门针对于Web的应用层拒绝服务攻击，攻击者操纵网络上的肉鸡，对目标Web服务器进行海量http request攻击，直到服务器带宽被打满，造成了拒绝服务。

慢速HTTP拒绝服务攻击经过不断的演变和发展，主要有三种攻击类型，分别是Slow headers、Slow body、Slow read。以Slow headers为例，Web应用在处理HTTP请求之前都要先接收完所有的HTTP头部，因为HTTP头部中包含了一些Web应用可能用到的重要的信息。攻击者利用这点，发起一个HTTP请求，一直不停的发送HTTP头部，消耗服务器的连接和内存资源。抓包数据可见，攻击客户端与服务器建立TCP连接后，每40秒才向服务器发送一个HTTP头部，而Web服务器再没接收到2个连续的\r\n时，会认为客户端没有发送完头部，而持续的等等客户端发送数据。如果恶意攻击者客户端持续建立这样的连接，那么服务器上可用的连接将一点一点被占满，从而导致拒绝服务。这种攻击类型称为慢速HTTP拒绝服务攻击。

**2 原理**

是以极低的速度往服务器发送HTTP请求。由于Web Server对于并发的连接数都有一定的上限，因此若是恶意地占用住这些连接不释放，那么Web Server的所有连接都将被恶意连接占用，从而无法接受新的请求，导致拒绝服务。

要保持住这个连接，RSnake构造了一个畸形的HTTP请求，准确地说，是一个不完整的HTTP请求。

        GET / HTTP/1.1\r\n

        HOST: host\r\n

        User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.503l3; )\r\n

        Content-Length: 42\r\n

在正常的HTTP包头中，是以两个CLRF表示HTTP Headers部分结束的。

由于Web Server只收到了一个\r\n，因此将认为HTTP Headers部分没有结束，并保持此连接不释放，继续等待完整的请求。此时客户端再发送任意HTTP头，保持住连接即可。

X-a: b\r\n

当构造多个连接后，服务器的连接数很快就会达到上限。

**3 安全加固**

如果是TOMCAT的话，

修改/conf/server.xml 配置中的connectionTimeout参数，修改为，7000ms或更少

原来：

<Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="8443" />

修改为：

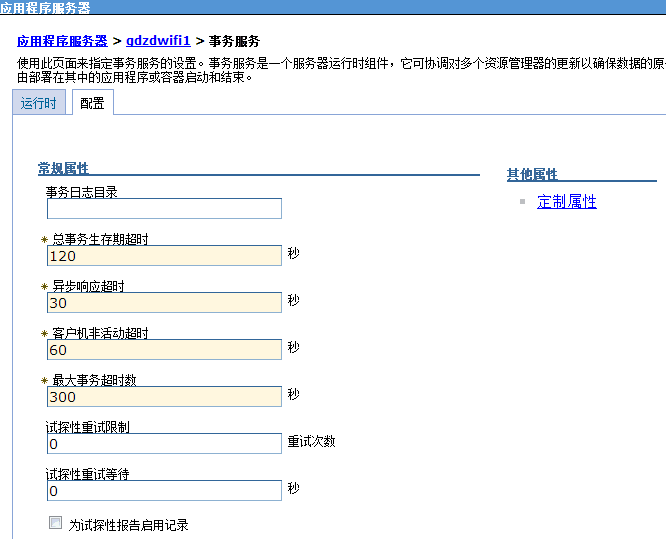
<Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="7000"

redirectPort="8443" />

案例二：

如果是WebSphere这个中间件的话



把异步响应超时改为7秒。

