## 中间件漏洞及修复汇总

1. ****Nginx文件解析漏洞****

****漏洞等级：高危****

****漏洞描述：****

nginx文件解析漏洞产生的原因是网站中间键版本过低，可将任意文件当作php可执行文件来执行，可导致攻击者执行恶意代码来控制服务器。

### ****漏洞危害：****

机密数据被窃取；

核心业务数据被篡改；

网页被篡改；

数据库所在服务器被攻击变为傀儡主机，导致局域网(内网)被入侵。

### ****修复方案：****

升级中间件版本

部署Web应用防火墙

对数据库操作进行监控

修改php.ini文件，将cgi.fix\_pathinfo的值设置为0；

在Nginx配置文件中添加以下代码：

 if( $fastcgi\_script\_name  
 ~ ..\*/.\*php   
 ) {return 403;}

这行代码的意思是当匹配到类似test.jpg/a.php的URL时，将返回403错误代码。

1. ****OPTIONS漏洞****

### ****漏洞描述：****

启用了不安全的http方法，Web服务器或应用程序服务器中间件是以不安全的方式配置 ，这些方法可能标识在服务器上启用了WebDAV，可能允许未授权的用户进行利用。此漏洞存在于IIS容器下，它扩展了HTTP协议，在GET/POST/HEAD等几个HTTP标准方法以外添加了一些新的方法，比如PUT/MOVE/COPY/DELETE方法，那么攻击者就可以通过PUT方法向服务器上传危险脚本。

### ****漏洞测试：****

请求一个OPTIONS包，查看服务器所支持的HTTP方法。

OPTIONS / HTTP/1.1

Host:thief.one

### ****漏洞危害：****

可能会在WEB服务器上上传、修改或删除WEB页面、脚本和文件，从而达到网页篡改，控制服务器的目的。

### ****漏洞修复方案：****

如果服务器不需要支持WebDAV，请务必禁用此功能，或者禁止其不安全的HTTP请求方法。

1. ****Struts2远程命令执行****

Struts2远程命令执行漏洞是指代码未对用户可控参数做过滤，导致直接带入执行命令的代码中，可被用来执行任意命令。

### ****可带来如下危害：****

攻击者可利用此漏洞直接执行操作系统命令获取WebShell，并且可通过该系统影响内网安全；

可被攻击者用来执行任意命令，写入后门等，进而完全控制服务器，造成严重后果。

**修复建议：**

将struts版本升级至最新版；

部署Web应用防火墙。

1. ****Tomcat远程部署漏洞****

### ****漏洞描述：****

这是JSP/PHP网站远程部署的一个工具，管理员只需要远程上传一个WAR格式的文件，便可以发布到网站，方便了开发人员部署代码的同时，也为黑客上传木马敞开了大门。

### ****漏洞验证：****

通过访问：Http://localhost:8080/manager管理地址，尝试弱口令或默认口令，若能登陆成功，则存在此漏洞。

### ****漏洞危害：****

导致被上传木马文件，控制服务器

### ****漏洞修复：****

1.删除此管理页面

2.防火墙设置外网禁止访问此页面，或设置上传文件类型

3.中间件设置此页面访问权限

4.修改默认账号密码

5.升级tomcat为最新版本

1. ****JBoss远程部署漏洞****

### ****漏洞描述：****

JBoss这是一个基于JavaEE的应用服务器，与tomcat类似的是jboss也有远程部署平台，但不需要登陆。

### ****漏洞验证：****

尝试访问http://localhost:8080 因为一般管理后台为8080端口

### ****漏洞危害：****

上传恶意木马文件，控制服务器

### ****漏洞修复：****

1.开启jmx-console密码认证

2.删除jmx-console.war与web-console.war

1. ****WebLogic远程部署漏洞****

### ****漏洞描述：****

weblogic是一个基于JavaEE构架的中间件，安装完weblogic默认会监听7001端口，可以用来远程部署网站代码。

### ****漏洞验证：****

默认后台地址：

http://localhost:7001/console/login/loginForm.jsp

### ****漏洞危害：****

可上传恶意木马文件，控制服务器

### ****漏洞修复：****

删除远程部署页面

1. ****Apache解析漏洞****

### ****漏洞描述：****

Apache 解析文件的规则是从右到左开始判断解析,如果后缀名为不可识别文件解析,就再往左判断。比如 test.php.owf.rar “.owf”和”.rar” 这两种后缀是apache不可识别解析,apache就会把wooyun.php.owf.rar解析成php

### ****漏洞检测：****

本地访问http://localhost/test.php.nmask，是否能被解析成php，若能则存在此漏洞。

### ****漏洞危害：****

配置文件上传漏洞，可绕过waf／黑名单等限制，上传木马文件，控制服务器。

### ****漏洞修复：****

1.apache配置文件，禁止.php.这样的文件执行，配置文件里面加入

<Files ~ “.(php.|php3.)”>  
        Order Allow,Deny  
        Deny from all  
</Files>

2.用伪静态能解决这个问题，重写类似.php.\*这类文件，打开apache的httpd.conf找到LoadModule rewrite\_module modules/mod\_rewrite.so把#号去掉，重启apache,在网站根目录下建立.htaccess文件,代码如下:

<IfModule mod\_rewrite.c>  
RewriteEngine On  
RewriteRule .(php.|php3.) /index.php  
RewriteRule .(pHp.|pHp3.) /index.php  
RewriteRule .(phP.|phP3.) /index.php  
RewriteRule .(Php.|Php3.) /index.php  
RewriteRule .(PHp.|PHp3.) /index.php  
RewriteRule .(PhP.|PhP3.) /index.php  
RewriteRule .(pHP.|pHP3.) /index.php  
RewriteRule .(PHP.|PHP3.) /index.php  
</IfModule>

1. ****Apache slowloris漏洞****

### ****漏洞描述：****

由于apache漏洞引发的拒绝服务攻击，其原理是以极低的速度往服务器发送HTTP请求。apache等中间件默认会设置最大并发链接数，而这种攻击就是会持续保持连接，导致服务饱和不可用。slowloris有点类似基于HTTP协议的SYN flood攻击。

### ****漏洞检测：****

slowhttptest工具

### ****漏洞危害：****

导致服务不可用，拒绝服务

### ****漏洞修复：****

1.升级apache为最新版本

2.针对ip+cookie，限制访问频率（由于cookie可以更改，ip可以使用代理，或者肉鸡，也不可靠)

3.关闭apache最大连接数等，合理配置中间件，缓解ddos攻击。

1. ****IIS6.0远程命令执行漏洞（cve-2017-7269）****

### ****漏洞描述：****

当IIS6.0 开启了WebDav协议（开启PROPFIND协议）时存在此漏洞，缓冲区溢出导致远程命令执行。

### ****漏洞检测：****

基于版本，windowsserver2003 R2+iis6.0+开启PROPFIND协议的服务器存在此漏洞。

### ****漏洞危害：****

服务器可被远程命令执行

### ****漏洞修复：****

1.关闭WebDAV服务

2.使用相关防护设备

1. ****IIS短文件名暴力猜解****

### ****漏洞描述：****

为了兼容16位MS-DOS程序，Windows为文件名较长的文件（和文件夹）生成了对应的windows 8.3 短文件名，而生成的短文件名符合一定的规律，可以被暴力猜解。

### ****漏洞检测：****

需要使用到通配符\*，在windows中，\*可以匹配n个字符，n可以为0。判断某站点是否存在IIS短文件名暴力破解漏洞，可以分别访问如下两个URL:

http://localhost/\\*~1\\*\\*\\*\\*/a.aspx

http://localhost/l1j1e\\*~1\\*\\*\\*\\*/a.aspx

这里我使用了4个星号，主要是为了程序自动化猜解，逐个猜解后缀名中的3个字符，实际上，一个星号与4个星号没有任何区别（上面已经提到，\*号可以匹配空）。

如果访问第一个URL，返回404。而访问第二个URL，返回400。 则目标站点存在漏洞。

### ****漏洞危害：****

猜解后台地址

猜解敏感文件，例如备份的rar、zip、.bak、.SQL文件等。

在某些情形下，甚至可以通过短文件名web直接下载对应的文件。比如下载备份SQL文件。

### ****漏洞修复：****

升级.net framework

修改注册表键值：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem

修改NtfsDisable8dot3NameCreation为1。再新建文件夹，将原网站目录内容拷贝进入新建的文件夹，使用新建的文件夹作为网站目录。

1. ****java反序列化漏洞****

### ****漏洞描述：****

由于某些java容器（中间件）中的jar包存在反序列化漏洞，导致可被远程命令执行。影响容器有：jenkins，jboss，weblogic，websphere等。

### ****漏洞检测：****

下载反序列化测试工具

### ****漏洞危害：****

导致服务器被远程命令执行

### ****漏洞修复：****

1.JBOSS

JBoss服务专有用户权限，没有登录权限，达到权限最小化,启用防火墙,防护防火墙策略设置，限定可以连接到JBoss的IP,安全验证配置,若是公开服务，需要在jmx-invoker-service.xml中开启权限验证,更新源代码,在JBoss源代码中打入最新的官方patch。

2.Weblogic

首先停止weblogic，在中间件modules目录下找到名为

com.bea.core.apache.commons.collections\_x.x.x.jar文件

然后下载最新的commons-collections(bin包)，用压缩包中的commons-collections-x.x.x.jar替换有漏洞的jar包

jar包下载地址：

http://commons.apache.org/proper/commons-collections/download\_collections.cgi

注意：保持原jar包的名字，即名字不变换掉jar包

最后启动weblogic。

1. ****Apache 默认页面泄漏漏洞****

### ****漏洞描述：****

Apache在安装后存在默认目录/icons/、/manual/

### ****漏洞检测：****

在浏览器里输入

http://IP/icons/，http://IP/manual/

如果能访问，则说明存在默认页面泄漏漏洞，如下图所示：



### ****修复方案：****

1.对于Apache2，注释掉Apache配置文件中的目录配置中的以下两行：

Alias /icons/ "/usr/share/apache2/icons/"  
AliasMatch ^/manual(?:/(?:de|en|es|fr|ja|ko|ru))?(/.\*)?$ "/usr/share/apache2/manual$1"

2.或者删除配置文件中的icons、manual两个目录。