Web 应用防火墙

服务公告

文档版本 01

发布日期 2022-05-12

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 Java Spring 框架远程代码执行高危漏洞

Spring是一款主流的Java EE轻量级开源框架，面向服务器端开发设计。近日，Spring框架被曝出可导致RCE远程代码执行的漏洞，该漏洞攻击面较广，潜在危害严重，对JDK 9及以上版本皆有影响。

漏洞名称

Spring框架RCE 0day安全漏洞

影响范围

- JDK 9及以上的。
- 使用了Spring框架或衍生框架。

防护建议

步骤1 **购买WAF**。

步骤2 将网站域名添加到WAF中并完成域名接入，详细操作请参见**添加防护域名**。

步骤3 将Web基础防护的状态设置为“拦截”模式，详细操作请参见**配置Web基础防护规则**。

图 1-1 Web 基础防护页面

须知

目前，该漏洞存在两种攻击payload，是否开启“header全检测”根据攻击payload的方式而定：

- 第一种是通过在参数提交中携带攻击载荷。此时，“header全检测”可以不开启拦截。
- 第二种是在header自定义字段中携带攻击载荷。此时，“header全检测”必须开启拦截模式，才可以拦截此类攻击。

第二种攻击方式对第一种有依赖，所以是否要开启“header全检测”，您可以根据您的业务需求进行选择。

----结束

2 Apache Dubbo 反序列化漏洞

2020年02月10日，华为云安全团队监测到Apache Dubbo官方发布了CVE-2019-17564漏洞通告，漏洞等级中危。当用户选择http协议进行通信时，攻击者可以通过发送POST请求的时候来执行一个反序列化的操作，由于没有任何安全校验，该漏洞可以造成反序列化执行任意代码。目前，华为云Web应用防火墙（Web Application Firewall，WAF）提供了对该漏洞的防护。

影响的版本范围

漏洞影响的Apache Dubbo产品版本包括： 2.7.0～2.7.4、2.6.0～2.6.7、2.5.x的所有版本。

安全版本

Apache Dubbo 2.7.5版本。

解决方案

建议您将Apache Dubbo升级到2.7.5版本。

如果您无法快速升级版本，或者希望防护更多其他漏洞，可以使用华为云Web应用防火墙对该漏洞进行防护，请参照以下步骤进行防护：

步骤1 **购买WAF**。

步骤2 将网站域名添加到WAF中并完成域名接入，详细操作请参见**添加防护域名**。

步骤3 将Web基础防护的状态设置为“拦截”模式，详细操作请参见**配置Web基础防护规则**。

----结束

3 开源组件 Fastjson 拒绝服务漏洞

2019年09月03日，华为云安全团队检测到应用较广的开源组件Fastjson的多个版本出现拒绝服务漏洞。攻击者利用该漏洞，可构造恶意请求发给使用了Fastjson的服务器，使其内存和CPU耗尽，最终崩溃，造成用户业务瘫痪。目前，华为云Web应用防火墙（Web Application Firewall，WAF）提供了对该漏洞的防护。

影响的版本范围

漏洞影响的产品版本包括：Fastjson 1.2.60以下版本，不包括Fastjson 1.2.60版本。

安全版本

Fastjson 1.2.60版本。

官方解决方案

建议用户将开源组件Fastjson升级到1.2.60版本。

防护建议

WAF支持对该漏洞的检测和防护，步骤如下：

步骤1 **购买WAF**。

步骤2 将网站域名添加到WAF中并完成域名接入，详细的操作请参见**添加防护域名**。

步骤3 将Web基础防护的状态设置为“拦截”模式，具体方法请参见**配置Web基础防护规则**。

----结束

4 开源组件 Fastjson 远程代码执行漏洞

2019年07月12日，华为云应急响应中心检测到开源组件Fastjson存在远程代码执行漏洞，此漏洞为2017年Fastjson 1.2.24版本反序列化漏洞的延伸利用，可直接获取服务器权限，危害严重。

影响的版本范围

漏洞影响的产品版本包括：Fastjson 1.2.51以下的版本，不包括Fastjson 1.2.51版本。

安全版本

Fastjson 1.2.51版本及以上的版本。

官方解决方案

建议用户将开源组件Fastjson升级到1.2.51版本或者最新的1.2.58版本。

防护建议

华为云Web应用防火墙内置的防护规则支持对该漏洞的防护，参照以下步骤进行防护：

步骤1 **购买WAF**。

步骤2 将网站域名添加到WAF中并完成域名接入，详细的操作请参见**添加防护域名**。

步骤3 将Web基础防护的状态设置为“拦截”模式，具体方法请参见**配置Web基础防护规则**。

----结束

5 Oracle WebLogic wls9-async 反序列化远程命令执行漏洞（CNVD-C-2019-48814）

2019年04月17日，华为云应急响应中心检测到国家信息安全漏洞共享平台（China National Vulnerability Database，CNVD）发布的Oracle WebLogic wls9-async组件安全公告。Oracle WebLogic wls9-async组件在反序列化处理输入信息时存在缺陷，攻击者可以发送精心构造的恶意HTTP请求获取目标服务器权限，在未授权的情况下远程执行命令，CNVD对该漏洞的综合评级为“高危”。

漏洞编号

CNVD-C-2019-48814

漏洞名称

Oracle WebLogic wls9-async反序列化远程命令执行漏洞

漏洞描述

WebLogic wls9-async组件存在缺陷，通过WebLogic Server构建的网站存在安全隐患。攻击者可以构造HTTP请求获取目标服务器的权限，在未授权的情况下远程执行命令。

影响范围

- Oracle WebLogic Server 10.X
- Oracle WebLogic Server 12.1.3

官方解决方案

官方暂未发布针对此漏洞的修复补丁。

防护建议

通过WAF的精准访问防护功能，参考**图5-1**和**图5-2**分别配置限制访问路径前缀为/_async/和/wls-wsat/的请求，拦截利用该漏洞发起的远程命令执行攻击请求。精准访问防护规则的具体配置方法请参见**配置精准访问防护规则**。

图 5-1 async 配置

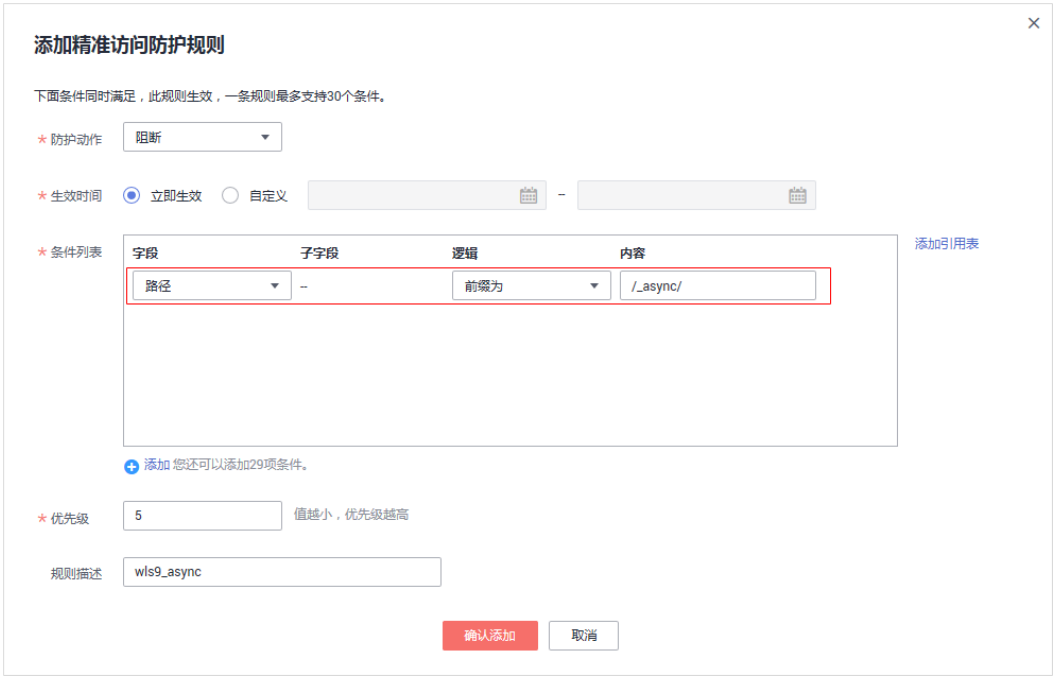

图 5-2 wls-wsat 配置