ALIBABA CLOUD

阿里云

Web应用防火墙

动态与公告

文档版本：20201016

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.防护引擎全面升级

自2020年3月11日起，Web应用防火墙将陆续为所有老用户全面升级防护引擎，为您提供更全面的防护能力和更便捷的操作体验。

升级至新版防护引擎后，您将获得以下体验升级：

- 防护体验全面升级

  分类聚合后的防护模块，从Web入侵防护、数据安全、Bot管理、访问控制/限流等多维度为您的业务提供全面防护。

  同时，更强大的精准限流能力和账户安全防护能力，帮助您有效抵御非法流量访问、CC攻击、撞库、弱口令攻击、暴力破解等威胁。升级后的趋势分析报表，为您更直观地展示防护效果，安全可视。

- 自定义防护策略满足精细化限流需求

  自定义策略防护支持更多精准访问控制字段和规则数，为您提供复杂条件下的精准限流访问能力，满足各种业务场景下的非法访问请求限制管理。

  - 原自定义CC防护规则整合至自定义防护策略，提供更精准的限流能力。详细信息，请参见设置自定义防护策略。
  - 原精准访问控制规则中的特定流量放行配置调整至各防护功能模块对应的白名单规则配置，提供更便捷的合法流量配置方式。详细信息，请参见设置网站白名单。

- 更便捷的IP黑名单配置体验

  一键添加基于IP、IP段以及IP所属地域的黑名单，实现访问控制的快捷操作，方便您快速拦截特定流量。

防护模块级别的白名单策略、扫描防护报表、放行优先的规则生效顺序等更多功能，等您发现。更多详细信息，请参见网站防护（新版引擎）相关文档。

升级方法

我们将陆续为所有2020年1月前开通Web应用防火墙的老用户安排防护引擎升级。当后端防护引擎升级完成后，您登录Web应用防火墙控制台时将收到升级提示，单击**立即体验**即可享受全新防护引擎为您带来的体验升级。

2.新功能发布记录

本文介绍了Web应用防火墙的产品功能和对应的文档动态。

更多关于Web应用防火墙的产品动态信息，请参见产品动态。

2020年

发布日期	功能动态	发布说明	相关文档
2020-08-17	资产识别	新增资产安全评分和网站资产Web指纹信息，帮助您判断资产中是否存在高危0 day漏洞风险。 说明 资产识别模块支持检测的网站资源覆盖阿里云域名和非阿里云域名（非阿里云域名包括解析至非阿里云服务器的域名和线下IDC机房使用的域名）。	资产识别
2020-07-09	透明接入模式发布上线	源站服务器部署在具有公网IP的阿里云ECS实例的业务，支持使用透明接入模式接入Web应用防火墙。透明接入模式下，您无需修改域名DNS解析和设置源站保护，同时也不用改变源站的IP地址，即可直接牵引源站ECS的流量到Web应用防火墙进行防护。	ECS/SLB透明接入
2020-06-08	API安全模块发布上线	Web应用防火墙新增API安全模块。API安全模块适用于网站业务中有API集成的用户，支持定义API规范文件来防护恶意API请求，避免网站资产受到数据篡改、重放攻击等威胁。	开启API安全
2020-06-04	自定义防护规则组体验优化&总览页面功能优化	• 自定义防护规则组支持系统规则自动更新功能，提升自定义规则组的安全性和可用性。 • 总览页面支持查看0day高危漏洞防护规则详情和影响范围。	自定义防护规则组 查看总览信息
2020-05-20	大数据深度学习引擎功能优化	大数据深度学习引擎模块支持调节攻击概率阈值，实现不同业务的最佳防护效果。	设置大数据深度学习引擎

发布日期	功能动态	发布说明	相关文档
2020-05-18	支持Terraform能力	面向成熟大企业的运维需求，WAF全面支持Terraform，可以实现用代码管理维护WAF产品的基本操作，包括域名运维和策略管理。 说明 需要控制台手动操作的任务可以通过这个能力用程序来自动化完成，不仅高效而且不易出错。更多信息，请参见Terraform帮助文档。	无
2020-04-10	用户体验优化	总览数据下钻到安全报表，安全报表数据下钻到日志服务，完善运营数据闭环体验。 • 总览页面的防护统计数据支持下钻到安全报表，且URL请求次数排名中透出所属域名信息。 • 安全报表的访问控制/限流统计数据支持下钻到日志服务，且支持查看和编辑有命中记录的自定义访问控制规则。	查看总览信息 查看安全报表
2020-04-02	Bot管理防护能力上线发布	Web应用防火墙新增Bot管理和APP防护增值服务，满足自动化攻击、Bot流量智能防护，以及面向原生app端的可信通信、防机器脚本滥刷等安全防护。 说明 Bot管理和APP防护模块目前仅向2020年1月发布的新版防护引擎开放。如果您使用旧版防护引擎，建议您尽快完成防护能力升级。	设置Bot管理白名单 概述
2020-03-10	新版防护引擎升级引导发布	Web应用防火墙新版防护引擎开通存量用户升级引导功能，分批平滑帮助用户完成过渡升级。	防护引擎全面升级
2020-03-04	智能负载均衡防护能力上线发布	智能负载均衡接入防护能力提供多节点、多线路自动容灾能力，打造最优线路的低时延访问体验。	智能负载均衡接入能力
2020-02-14	日志服务升级和体验优化	Web应用防火墙日志服务功能升级优化，支持自定义域名快速开启全量日志等功能。	无
2020-02-10	事件告警能力全面升级	Web应用防火墙通过升级告警通知功能，聚焦基础数据和事件生成，支持了安全事件告警、业务监控告警，有效满足用户日常运维诉求。	配置告警监控

发布日期	功能动态	发布说明	相关文档
2020-01-15	应用防护能力全面升级	Web应用防火墙新一代防护引擎满足精细化限流防护需求，有效防护非法流量访问，同时支持账户安全防护，有效防御常见的CC攻击、撞库、弱口令等行为。 说明 防护能力对全部用户生效，控制台配置能力只针对新购用户，历史保有用户在3月份支持升级使用。	设置正则防护引擎

2019年

发布日期	功能动态	发布说明	相关文档
2019-12-20	独享版功能优化升级	Web应用防火墙独享版支持用户自定义配置域名的超时时长，优化功能体验。	设置独享集群
2019-11-28	账户安全检测能力发布	Web应用防火墙账户安全模块协助用户识别登录相关接口上发生的账户安全风险事件，包括撞库、暴力破解、垃圾注册、弱口令嗅探和短信验证码接口滥刷等。	设置账户安全
2019-10-25	虚拟化独享版发布	Web应用防火墙独享版支持基于业务防护端口、TLS加密版本和算法、拦截响应页面等定制防护能力，满足用户特殊业务的Web防护需求。	设置独享集群
2019-10-22	已防护网站资产URL画像功能发布	Web应用防火墙根据历史正常业务流量，协助用户自动化识别业务URL画像和业务量，方便执行和开通“千人千面”定制防护策略。	无
2019-10-16	总览页面透出防扫描防护能力	Web应用防火墙总览页面展示防扫描模块拦截总量、已拦截扫描攻击事件列表、扫描攻击事件详情和对应的安全专家处置建议。	查看总览信息
2019-09-24	资产管理支持一键添加应用防护的能力	Web应用防火墙资产管理页面展示已接入防护的资产的防护状态，并且支持一键添加资产到Web应用防火墙进行防护的能力。	资产识别
2019-08-22	主动防御能力发布	Web应用防火墙主动防护能力基于大数据智能学习算法，对用户历史业务流量不断迭代学习，建立“千人千面”的自动化防护策略。	设置主动防御
2019-07-30	云上网站资产管理功能发布	Web应用防火墙网站资产管理协助用户全面识别云上网站资产信息，完善网站一键接入防护能力，从而协助用户建立全面、安全的Web应用防御体系。	资产识别

发布日期	功能动态	发布说明	相关文档
2019-07-18	安全报表中增加Web攻击详情页面	Web应用防火墙安全报表中增加Web攻击详情页面，展示攻击拦截的具体原因，帮助用户提升安全运维效率和效果。	查看安全报表
2019-06-27	支持防护基于HTTP2协议的应用	Web应用防火墙支持基于HTTP2协议的应用流量防护，完善应用协议覆盖率，更全面地防护Web应用防火墙用户的应用业务。	添加域名
2019-06-13	防护配置中支持设置Web解码方式	Web应用防火墙防护配置中支持用户自定义配置Web解码方式。	设置正则防护引擎
2019-05-30	ACL规则优化	Web应用防火墙访问控制规则中支持添加多个IP或者IP地址段作为条件匹配内容。	设置自定义防护策略
2019-05-30	产品总览页面升级	Web应用防火墙总览页面支持基于海量日志聚合安全运营事件，并提供专家处置建议；提供分类统计攻击总量和TOP域名分布，提升产品的运营能力。	查看总览信息
2019-04-30	IPv6业务的应用防护能力发布	Web应用防火墙支持一键接入基于IPv6的源站业务系统，无需源站改造。IPv6业务接入即可支持防护，协助用户的IPv6业务系统满足等保合规要求。	开启IPv6防护
2019-03-19	防Web攻击扫描功能发布	Web应用防火墙提供Web扫描指纹的威胁情报库，支持用户自定义Web扫描的封禁频率和时长，并支持自动拦截目录遍历等常见扫描特征请求。	设置扫描防护
2019-03-15	透明接入模式发布	针对阿里云ECS用户提供一键接入Web应用防火墙的能力，无需变更DNS解析。目前仅支持华北2节点。	使用透明代理模式接入WAF
2019-01-03	区域IP封禁支持自定义全球指定国家、地区	Web应用防火墙的区域IP封禁功能支持封禁指定的全球国家/地区。	设置IP黑名单

2018年

发布日期	功能动态	发布说明	相关文档
2018-12-20	网页防篡改API发布	Web应用防火墙网页防篡改API发布，支持用户以API方式调用网页防篡改的常见操作，包括更新缓存、添加网页防篡改防护等。	无
2018-12-13	自定义Web防护规则组发布	Web应用防火墙自定义Web防护规则组发布，能够针对自身业务设置特定规则，避免默认规则误触发拦截，保障业务安全。	自定义防护规则组

发布日期	功能动态	发布说明	相关文档
2018-11-16	支持长达一年的业务日志存储	Web应用防火墙支持通过日志服务SLS的集成功能实时采集已接入Web应用防火墙防护的网站业务日志，并提供日志实时检索与分析服务。	使用全量日志
2018-10-24	支持流量标记功能	Web应用防火墙支持流量标记功能，允许用户在请求流量中插入特定头部值，方便标记由WAF转发的流量。	添加域名
2018-10-17	支持使用唯一ID在全量日志中查询拦截事件	Web应用防火墙支持使用唯一ID在全量日志中查询拦截事件，帮助用户快速定位拦截原因及请求详情。	使用全量日志
2018-10-01	支持安全事件告警	Web应用防火墙支持通过短信或邮件向您推送安全事件和系统告警，您可以自定义需要关注的业务指标，及时发现业务异常情况。	配置告警监控
2018-08-09	支持深度学习引擎	Web应用防火墙支持深度学习引擎，依靠强大的机器学习能力，识别异常风险并进行拦截。	设置大数据深度学习引擎
2018-07-27	OpenAPI发布	Web应用防火墙针对常见控制台配置操作开放对应API接口，方便用户执行批量化操作。	API概览
2018-05-29	推出业务数据大屏试用服务	Web应用防火墙推出业务数据大屏试用，方便用户在第一时间了解网站业务全貌。	数据大屏
2018-04-27	精准访问控制功能升级发布	Web应用防火墙支持使用更多的HTTP头部字段设置ACL规则，过滤访问请求。	设置自定义防护策略
2018-03-16	数据大屏公测发布	Web应用防火墙开放数据大屏服务，为安全运维人员提供重点数据监控和展示的功能。	数据大屏
2018-03-15	支持关闭实例	Web应用防火墙支持用户在控制台自主释放产品。	关闭WAF
2018-01-30	支持全量日志下载	Web应用防火墙在企业版及更高版本中提供全量访问日志的智能检索和下载功能。	使用全量日志
2018-01-11	“蚁盾”手机号风控服务发布	Web应用防火墙的“蚁盾”手机号风险评分可有效解决机器注册、恶意刷单、黄牛抢购等问题。 说明 该服务已下线。	无

2017年

发布日期	产品动态	发布说明

发布日期	产品动态	发布说明
2017-12-28	新增支持防护的非标端口	Web应用防火墙新增非标端口支持，支持更多非标准业务端口的防护。
2017-11-24	支持多种负载均衡算法	Web应用防火墙支持多种负载均衡算法，用户可以自主选择，应对不同场景的需求。
2017-10-30	提供App业务安全解决方案	Web应用防火墙提供App业务安全解决方案，解决App防刷、防爬需求。
2017-10-26	支持Websocket	Web应用防火墙支持网站Websocket业务接入。
2017-08-31	支持异常响应码监控	Web应用防火墙支持监控异常响应码。
2017-08-31	支持业务带宽查询	Web应用防火墙支持查询业务上下行的带宽使用量。
2017-08-31	支持业务QPS查询	Web应用防火墙支持实例级别及域名粒度的QPS查询。
2017-08-16	支持查看黑洞事件详情	Web应用防火墙支持查看黑洞发生时的攻击阈值、事件等信息。
2017-07-27	域名独享IP功能发布	Web应用防火墙支持设置域名独享IP。用户可以通过购买域名独享资源包实现域名的IP资源隔离。
2017-07-25	精准访问控制功能优化	Web应用防火墙精准访问控制规则中支持放行数据风控及区域封禁功能的策略。
2017-07-25	人机识别算法功能优化	Web应用防火墙优化了CC自定义规则中的人机识别算法，提升CC攻击的拦截率。
2017-07-25	规则支持更多逻辑符配置	Web应用防火墙的精准访问控制规则新增支持“该字段不存在”、“值长度范围”等逻辑配置。
2017-07-25	支持更多HTTP字段检测	Web应用防火墙在精准访问控制中支持对更多HTTP字段的规则配置。
2017-06-07	支持回源到域名	Web应用防火墙网站配置中支持填写域名格式的回源地址。
2017-05-25	防敏感信息泄露功能发布	Web应用防火墙配合网络安全法相关规定，推出敏感数据防护方案。
2017-04-12	支持网站一键HTTPS	Web应用防火墙支持网站一键HTTPS化，无需用户更改服务器配置。
2017-04-12	多版本支持非标准端口防护	非标准的部分端口业务在Web应用防火墙的多个版本中得到支持，可以实现安全防护。
2017-03-28	大数据威胁情报功能发布	Web应用防火墙大数据威胁情报功能提供安全体检分评估、高危风险预警、黑客真人攻击详情查看等服务。
2017-03-08	接入体验优化	Web应用防火墙域名添加中支持一键解析DNS。

发布日期	产品动态	发布说明
2017-02-09	网页防篡改功能发布	Web应用防火墙具备网页防篡改能力，避免网页的恶意篡改。
2017-02-09	全量日志搜索功能发布	Web应用防火墙支持全量业务访问日志一键搜索。
2017-01-05	支持虚拟主机接入	Web应用防火墙支持接入万网虚拟主机进行网站防护。

2016年

发布日期	产品动态	发布说明
2016-12-21	V3.1版本重磅发布	Web应用防火墙V3.1版本发布，重点提升引擎核心防护能力，新增地理区域IP封禁、CC规则自定义配置等功能。
2016-12-01	智能语义分析引擎上线	Web应用防火墙防护引擎新增智能语义分析功能，相比较现有的基于正则的规则，在误漏报率上有显著提升。

3.安全公告

3.1. FastJSON远程代码执行0day漏洞（2019-7-23）

2019年7月23日，阿里云云盾应急响应中心监测到FastJSON存在0day漏洞，攻击者可以利用该漏洞绕过黑名单策略进行远程代码执行。

漏洞名称

FastJSON远程代码执行0day漏洞

漏洞描述

利用该0day漏洞，恶意攻击者可以构造绕过FastJSON黑名单策略补丁的攻击请求，进行远程代码执行攻击。例如，攻击者通过精心构造的请求，绕过FastJSON黑名单策略补丁远程让服务端执行指定命令（以下示例中成功运行计算器程序）。

影响范围

- FastJSON 1.2.24及以下版本
- FastJSON 1.2.41至1.2.45版本

官方解决方案

升级至FastJSON最新版本，建议升级至1.2.58版本。

> **说明** 强烈建议不在本次影响范围内的低版本FastJSON也进行升级。

升级方法

您可以通过更新Maven依赖配置，升级FastJSON至最新版本（1.2.58版本）。

```
<dependency>
 <groupId>com.alibaba</groupId>
 <artifactId>fastjson</artifactId>
 <version>1.2.58</version>
</dependency>
```

防护建议

Web应用防火墙的Web攻击防护规则中已默认配置相应规则防护该FastJSON 0day漏洞，启用Web应用防火墙的Web应用攻击防护功能即可。

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请关注安全管家服务。

3.2. FastJSON远程代码执行0day漏洞（2019-6-22）

2019年6月22日，阿里云云盾应急响应中心监测到FastJSON存在0day漏洞，攻击者可以利用该漏洞绕过黑名单策略进行远程代码执行。

漏洞名称

FastJSON远程代码执行0day漏洞

漏洞描述

利用该0day漏洞，恶意攻击者可以构造攻击请求绕过FastJSON的黑名单策略。例如，攻击者通过精心构造的请求，远程让服务端执行指定命令（以下示例中成功运行计算器程序）。

影响范围

FastJSON 1.2.48以下版本

官方解决方案

升级至FastJSON最新版本，建议升级至1.2.58版本。

> 说明 强烈建议不在本次影响范围内的低版本FastJSON也进行升级。

升级方法

您可以通过更新Maven依赖配置，升级FastJSON至最新版本（1.2.58版本）。

```
<dependency>
 <groupId>com.alibaba</groupId>
 <artifactId>fastjson</artifactId>
 <version>1.2.58</version>
</dependency>
```

防护建议

Web应用防火墙的Web攻击防护规则中已默认配置相应规则防护该FastJSON 0day漏洞，启用Web应用防火墙的Web应用攻击防护功能即可。

> 说明 如果您的业务使用自定义防护规则组功能自定义所应用的防护规则，请务必在自定义规则组中添加以下规则：

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请关注安全管家服务。

3.3. Consul Service API远程命令执行漏洞

2018年11月27日，Consul在官方博客中发布了关于Consul工具在特定配置下可能导致远程命令执行（RCE）漏洞的公告，并描述了防护该漏洞的配置方案。

Consul是HashiCorp公司推出的一款开源工具，用于实现分布式系统的服务发现与配置。同其他分布式服务注册与发现的方案相比，Consul提供的方案更为一站式。Consul内置了服务注册与发现框架、分布一致性协议实现、健康检查、Key-Value存储、多数据中心方案，不再需要依赖其他工具（例如ZooKeeper等），使用方式也相对简单。

Consul使用Go语言编写，因此具有天然的可移植性（支持Linux、Windows和Mac OS X系统），且安装包中仅包含一个可执行文件，便于部署，可与Docker等轻量级容器无缝配合。

漏洞名称

Hashicorp Consul Service API远程命令执行漏洞。

漏洞描述

在特定配置下，恶意攻击者可以通过发送精心构造的HTTP请求在未经授权的情况下在Consul服务端远程执行命令。关于该Consul漏洞的更多详细信息，请参见HashiCorp官方公告。

漏洞复现过程：

1. 验证Consul服务端存在该远程命令执行漏洞。

   

2. 构造HTTP PUT请求，实现在Consul服务端远程执行命令。

   

影响范围

启用了脚本检查参数（-enable-script-checks）的所有版本。

防护建议

您可以通过选择以下适合的方案防护该Consul漏洞：

- 禁用Consul服务器上的脚本检查功能。
- 如果您需要使用Consul的脚本检查功能，请升级至0.9.4、1.0.8、1.1.1、1.2.4中的任意一个版本（这些版本中包含-enable-local-script-checks参数），将Consul配置中的-enable-script-checks更改为-enable-local-script-checks。
- 确保Consul HTTP API服务无法通过外网访问或调用。
- 启用Web应用防火墙的自定义防护策略功能，配置以下防护规则，表示阻断所有使用了HTTP PUT方法，且访问URL中包含 `/v1/agent/service/register` 的访问请求。具体操作请参见设置自定义防护策略。

  

更多信息

您还可以使用安全管家服务。安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请参见安全管家服务。

3.4. Apache Solr远程反序列化代码执行漏洞（CVE-2019-0192）

2019年3月7日，阿里云云盾应急响应中心监测到Apache官方发布的关于Solr的安全公告。通过调用Config API修改jmx.serviceUrl属性指向恶意的RMI服务，导致Apache Solr出现远程反序列化代码执行的安全漏洞。

漏洞编号

CVE-2019-0192

漏洞名称

Apache Solr jmx.serviceUrl远程反序列化代码执行漏洞

漏洞描述

Config API接口允许通过发送HTTP POST请求配置Apache Solr的JMX服务器，修改jmx.serviceUrl的属性。恶意攻击者通过将其指向恶意的RMI服务器，可以利用Solr的不安全的反序列化触发远程代码执行。

影响范围

- Apache Solr 5.00至5.5.5版本
- Apache Solr 6.00至6.6.5版本

官方解决方案

- 将您的Apache Solr升级至7.0或以上版本。
- 通过修改配置 `disable.configEdit=true` ，禁用Config API接口。
- 在网络层确保仅放行受信任的流量访问Solr服务器。

如果升级版本或禁用Config API都不可行，请申请官方补丁并重新编译Solr。

防护建议

如果您暂时不希望通过升级Solr版本解决该漏洞，建议您使用Web应用防火墙的精准访问控制功能对您的业务进行防护。

通过精准访问控制功能，限制包含特定JSON数据（service:jmx:rmi）的POST请求，拦截利用该漏洞发起的远程代码执行攻击请求。

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请关注安全管家服务。

3.5. Jenkins任意文件读取漏洞（CVE-2018-1999002）

2018年7月18日（美国时间），Jenkins官方发布最新安全通告，披露多个安全漏洞。其中，SECURITY-914是由Orange发现的Jenkins未授权任意文件读取漏洞，存在高危风险。

利用该漏洞，攻击者可以读取Windows系统服务器中的任意文件，且在特定而条件下也可以读取Linux系统服务器中的文件。通过利用该文件读取漏洞，攻击者可以获取Jenkins系统的凭证信息，导致用户的敏感信息遭到泄露。同时，Jenkins的部分凭证可能与其用户的帐号密码相同，攻击者获取到凭证信息后甚至可以直接登录Jenkins系统进行命令执行操作等。

漏洞编号

CVE-2018-1999002

漏洞名称

Jenkins任意文件读取漏洞

漏洞描述

在Jenkins的Stapler Web框架中存在任意文件读取漏洞。恶意攻击者可以通过发送精心构造的HTTP请求在未经授权的情况下获取Jenkin主进程可以访问的Jenkins文件系统中的任意文件内容。

关于该漏洞更多信息，请查看官方漏洞公告。

影响范围

- Jenkins weekly 2.132及此前所有版本
- Jenkins LTS 2.121.1及此前所有版本

官方解决方案

- 将您的Jenkins weekly升级至2.133版本。
- 将您的Jenkins LTS升级至2.121.2版本。

防护建议

如果您暂时不希望通过升级Jenkins版本解决该漏洞，建议您使用Web应用防火墙的精准访问控制功能对您的业务进行防护。

通过精准访问控制功能，针对Accept-Language这个HTTP请求头设置阻断规则过滤该请求头中包含 `../` 的请求，防止攻击者利用该漏洞通过目录穿越读取任意文件。

实际防护效果

通过配置上述精准访问控制规则，WAF成功阻断试图利用该漏洞的精心构造的HTTP请求。

> **说明** 关于精准访问控制规则的功能介绍，请查看精准访问控制。

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请关注安全管家服务。

3.6. Apache Struts2 REST插件DoS漏洞（CVE-2018-1327）防护最佳实践

HPE的两名安全专家（Yevgeniy Grushka和Alvaro Munoz）发现Apache Strust2的REST插件中存在DoS漏洞。如果您在Struts REST插件中使用XStream类库处理程序，攻击者可以构造恶意的XML请求发起DoS攻击。

漏洞编号

CVE-2018-1327

漏洞名称

Apache Struts2 REST插件DoS漏洞（S2-056）

漏洞描述

S2-056漏洞存在于Apache Struts2的REST插件中。当使用XStream组件对XML格式的数据包进行反序列化操作，且未对数据内容进行有效验证时，攻击者可通过提交恶意的XML数据对应用发起远程DoS攻击。

当恶意攻击者发起大量攻击请求时，您的应用所在服务器的CPU资源将被迅速占满。

关于该漏洞更多信息，请查看官方漏洞公告。

影响范围

Struts 2.1.1 - Struts 2.5.14.1

官方解决方案

将您的Apache Struts升级至2.5.16版本。

防护建议

如果您暂时不希望通过升级Apache Struts版本解决该漏洞，建议您使用Web应用防火墙的精准访问控制和CC攻击自定义规则功能对您的业务进行防护。

- 通过精准访问控制功能，限制包含特定XML数据（`com.sun.xml.internal.ws.encoding.xml.XMLMessage$XmlDataSource`）的POST请求，阻断利用该漏洞发起的DoS攻击请求。例如，配置以下规则阻断在Apache Strust的REST插件中使用XStream类库应用页面的攻击请求。
- 通过CC攻击防护自定义功能，限制同一个IP对在Apache Strust的REST插件中使用XStream类库的应用页面的请求频率。例如，配置以下规则限制对指定页面的请求频率不超过每5秒100次。

关于精准访问控制和CC攻击防护自定义规则的功能介绍，请查看精准访问控制和自定义CC防护。

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请关注安全管家服务。

3.7. WordPress拒绝服务（CVE-2018-6389）漏洞防护最佳实践

2018年2月5日，国外安全研究人员披露了一个关于Wordpress的拒绝服务（DoS）攻击的漏洞（CVE-2018-6389），WordPress 3.x-4.x各个版本均受该漏洞影响。恶意攻击者可以通过让WordPress在单个请求中加载多个Javascript文件来消耗服务器资源，进而引发拒绝服务。

云盾WAF本身不受该漏洞影响。但如果您的网站业务使用WordPress，建议您配置相应的防护规则。

漏洞描述

该漏洞主要位于*load-scripts.php*文件处，*load-scripts.php*是WordPress CMS的内置脚本。*load-scripts.php*文件通过传递 `name` 到 `load` 参数来选择性地调用必需的Javascript文件，这些 `name` 参数间以”,”隔开。

例如，`https://example.com/wp-admin/load-scripts.php?c=1&load[]=jquery-ui-core,editor&ver=4.9.1`，这个请求中加载的Javascript文件是*jquery-ui-core*和*editor*。

由于在*script-loader.php*文件中定义的181个Javascript文件都可以被加载在单个请求中，恶意攻击者在无需授权登录的情况下可以发送大量请求，导致服务器负载增加，从而实现拒绝服务攻击的效果。

防护建议

建议您使用精准访问控制和CC攻击自定义规则功能对您的WordPress网站业务进行防护。

- 通过精准访问控制功能，限制向*load-scripts.php*文件传递参数的数量。例如，配置以下规则限制对*load-scripts.php*文件传递的参数长度不大于50个字符。
- 通过CC攻击防护自定义功能，限制同一个IP对*load-scripts.php*文件的请求频率。例如，配置以下规则限制对同一个IP对*load-scripts.php*文件的请求频率不超过每5秒100次。

关于精准访问控制和CC攻击防护自定义规则的功能介绍，请参见精准访问控制和自定义CC防护。

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请关注安全管家服务。

3.8. WordPress xmlrpc PingBack反射攻击防护最佳实践

本文用于在遭受WordPress反射攻击时，通过Web应用防火墙防御WordPress反射攻击。

什么是WordPress反射攻击

WordPress是一种使用PHP语言开发的博客平台，pingback是WordPress的一个插件。黑客可以利用pingback对网站发起WordPress反射攻击。

在遭受WordPress攻击后，您可以在服务器日志上看到大量User-Agent中包含WordPress、pingback字样的请求。

WordPress反射攻击是CC攻击的变种，可以造成网页加载极其缓慢、服务器CPU飙升、失去响应等情况。

关于攻击的原理，请参见WordPress反弹攻击那点事儿。

如何使用Web应用防火墙进行防御

1. 登录云盾Web应用防火墙控制台。
2. 前往**管理 > 网站配置**页面。
3. 选择需要防护的域名，单击其操作列下的**防护配置**。
4. 在**精准访问控制**下，单击**前去配置**。
5. 单击**新增规则**，分别添加以下两条精准访问控制规则。
   - 阻断User-Agent中包含pingback的访问。
     - **规则名称**：wp1
     - **匹配字段**：User-Agent
     - **逻辑符**：包含
     - **匹配内容**：pingback
     - **匹配动作**：阻断
   - 阻断User-Agent中包含WordPress的访问。
     - **规则名称**：wp2
     - **匹配字段**：User-Agent
     - **逻辑符**：包含
     - **匹配内容**：WordPress
     - **匹配动作**：阻断

> **说明** 两条规则要分开添加。

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效的应对漏洞及黑客攻击，详情请关注安全管家服务。