ALIBABA CLOUD

Alibaba Cloud

云防火墙
安全通告

文档版本：20210415

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.安全通告

2.【基础规则】PostgreSQL恶意文件写入攻击

阿里云云防火墙已支持防护PostgreSQL恶意文件写入攻击。

PostgreSQL是一个功能强大的开源、对象关系数据库管理系统，可以跨平台在多个操作系统上运行。PostgreSQL的 `lo_export` 自带函数可将大型对象导出到文件并通过SQL调用执行。此过程经常被攻击者利用，当攻击者拿到PostgreSQL的数据库权限后，就可以通过 `lo_import` 和 `lo_export` 函数导入恶意库文件，进而执行系统命令。

漏洞影响范围：PostgreSQL数据库

漏洞危险等级：高危

规则防护：云防火墙虚拟补丁已支持防护

规则类型：命令执行

3.【威胁情报】多个僵尸网络开始使用ThinkPHP v5漏洞

阿里云云防火墙可防御多个僵尸网络开始使用ThinkPHP v5漏洞。

近日，阿里云应急响应中心监控到以BuleHero和Sefa为代表的两个挖矿僵尸网络开始利用ThinkPHP框架的5.x远程命令执行漏洞进行传播。BuleHero是一个利用多种安全漏洞入侵和传播，进而控制服务器进行挖矿的僵尸网络，对正常业务构成重大安全威胁。存在ThinkPHP v5漏洞的系统易被感染，一旦感染BuleHero或Sefa，蠕虫会进行内网传播，对企业内网造成损失，还可控制服务器进行挖矿，影响业务正常运行。

部分下载URL及详情参见威胁预警-多个挖矿僵尸网络开始使用ThinkPHP v5漏洞。

漏洞危险等级：高危

规则防护：云防火墙虚拟补丁已支持防护

规则类型：蠕虫攻击

4.【虚拟补丁】ThinkPHP 5.x远程命令执行（getshell）

云防火墙已可防御ThinkPHP 5.x远程命令执行（getshell）攻击。

ThinkPHP是源自中国的一个简便快速、兼容性强的轻量级PHP开发框架，在中国使用较多，特别是电子商务行业、金融服务行业、互联网游戏行业等行业网站。

2018年12月10日，ThinkPHP v5系列发布安全更新，修复了一处可导致远程代码执行的严重漏洞。该漏洞覆盖面广，可直接远程执行任何代码和命令。由于ThinkPHP v5框架对控制器名未进行足够的安全检测，此漏洞可导致在没有开启强制路由的情况下，攻击者通过构造特定的请求，直接进行远程代码执行，进而获得服务器权限。

漏洞影响范围：ThinkPHP v5.0.0~5.0.23、ThinkPHP v5.1.0~5.1.31

漏洞危险等级：高危

规则防护：云防火墙虚拟补丁已支持防护

规则类型：Web攻击

5.【基础规则】Bash反弹shell检测规则更新

云防火墙已可防护Bash反弹shell检测规则更新攻击。

反弹shell是网络攻击中较多利用的一种攻击，攻击一般发生在攻击维持阶段。当攻击者已经拿到系统的部分命令执行权限后，就可以通过反弹shell拿到一个可交互的命令执行窗口，进而继执行后阶段的入侵和信息窃取。当云防火墙检测到反弹shell时，说明您的服务器正在遭受入侵风险，此时云防火墙会拦截反弹shell过程的建立及命令执行，防止攻击风险的进一步加剧。

漏洞危险等级：高危

规则防护：云防火墙虚拟补丁已支持防护

规则类型：反弹shell

6.【基础规则】矿池通信检测类规则更新

阿里云云防火墙已更新挖矿通信检测类规则。

随着以比特币为主的虚拟货币的兴起，受挖矿带来的直接经济收益的驱动，以挖矿为目的的安全事件日益猖獗，越来越多的服务器被入侵、进行虚拟货币挖矿。计算机一旦被挖矿木马感染，就会成为黑客的盈利工具，同时计算机的资源也会被耗尽，对正常业务造成严重的影响。近日，云防火墙已更新挖矿通信检测类规则，可检测服务器是否存在虚拟货币挖矿行为。

漏洞危险等级：高危

规则防护：云防火墙虚拟补丁已支持防护

规则类型：挖矿行为

7.【基础规则】Phpcms2008代码注入漏洞（CVE-2018-19127）

Phpcms网站内容管理系统是中国主流CMS系统之一，同时也是一个开源的PHP开发框架。由于Phpcms稳定、灵活、开源的特性，时至今日，Phpcms 2008版本仍被许多网站所使用。Phpcms 2008存在代码注入漏洞，漏洞编号为CVE-2018-19127。攻击者可向网站上路径可控的缓存文件写入任意内容，从而可能获取webshell并执行任意指令。

阿里云安全近日已捕获到Phpcms 2008代码注入漏洞的多个利用样本。

漏洞影响范围：Phpcms 2008

漏洞危险等级：高危

规则防护：云防火墙虚拟补丁已支持防护

规则类型：命令执行

8.【虚拟补丁】WebLogic T3协议反序列化漏洞

Oracle官方发布了4月份的关键补丁更新CPU（Critical Patch Update），其中包含一个高危的WebLogic T3协议反序列化漏洞（CVE-2018-2628），通过该漏洞攻击者可以在未授权的情况下构造恶意请求报文远程执行命令获取系统权限，带来严重的安全风险。Oracle官方及时发布了最新补丁修复了该漏洞，阿里云安全团队建议您尽快自查并升级。

漏洞影响范围：WebLogic 10.3.6.0、WebLogic 12.1.3.0、WebLogic 12.2.1.2、WebLogic 12.2.1.3

漏洞危险等级：高危

规则防护：防护漏洞导致的远程命令执行

规则类型：命令执行

9.【威胁情报】Redis未授权访问攻击信息

2018年9月12日监控到大量利用Redis未授权访问的蠕虫传播事件，攻击源为被蠕虫感染的主机。

中控IP：104.20.208.21

受控后会访问恶意源hxxps://pastebin.com/raw/5bjpjvLP下载恶意文件，并会利用受控端接收攻击IP段后继续传播。

恶意IP：104.20.208.21

漏洞危险等级：高危

事件：Redis蠕虫中控

10.【基础规则】Microsoft SQL Server xp_cmdshell远程命令执行

SQL Server是Microsoft公司推出的关系型数据库管理系统。xp_cmdshell是SQL Server运行系统命令行的系统存储过程，该选项使系统管理员能够控制是否可以在系统上生成Windows命令shell并以字符串的形式传递以便执行，执行结束的任何输出都作为文本的行返回。被攻击者恶意利用可能导致以SQL Server运行权限执行系统命令。

漏洞影响范围：Microsoft SQL Server

漏洞危险等级：高危

规则防护：防护由SQL Server xp_cmdshell导致的远程命令执行

规则类型：命令执行

11.【虚拟补丁】Nginx安全问题易导致DoS攻击

近日Nginx被爆出存在安全问题，可能会导致1400多万台服务器遭受DoS攻击。导致安全问题的漏洞存在于HTTP/2和MP4模块中。

Nginx HTTP/2实现中发现了两个安全漏洞。如果在配置文件中使用**listen**指令的**http2**选项，会影响使用ngx_http_v2_module编译的Nginx（默认情况下不编译），可能导致过多的内存消耗（CVE-2018-16843）和CPU使用率（CVE-2018-16844）。具体请参见Nginx 安全问题致使 1400 多万台服务器易遭受 DoS 攻击。

为了利用上述两个漏洞，攻击者可以发送特制的HTTP/2 请求，这将导致过多的CPU使用和内存使用，最终触发DoS状态。所有运行未打上补丁的Nginx服务器都容易受到DoS攻击。

漏洞影响范围：

- CVE-2018-16843和CVE-2018-16844影响的版本：Mainline version 1.9.5~1.15.5
- CVE-2018-16845影响的版本：Mainline version 1.1.3+、1.0.7+

漏洞危险等级：高危

规则防护：云防火墙虚拟补丁已支持防护

规则类型：DoS攻击

12.【威胁情报】QBotVariant蠕虫网络攻击情报

阿里云安全在今年5月份监测到了一种改写自互联网公开渠道源码的蠕虫样本，我们将该类样本命名为QBot Variant。QBot Variant具有DDoS攻击、后门、下载器和破解等功能，一旦感染此类蠕虫，不仅会占用主机计算资源消耗带宽流量，成为攻击其他主机的肉鸡，还可能造成数据泄露、数据丢失等后果。QBot Variant可在互联网上广泛传播并造成极大的危害。

QBot Variant传播的方式有以下两种：

- 利用Hadoop Yarn资源管理系统的REST API未授权访问漏洞进行入侵。
- 通过硬编码的弱密码进行SSH暴力破解。

漏洞危险等级：高危

规则防护：云防火墙虚拟补丁已支持防护

事件：蠕虫攻击

13.【威胁情报】DDG僵尸网络攻击情报

DDG是一个主要通过SSH爆破、Redis未授权访问等漏洞进行传播，并攫取服务器算力挖矿（门罗币）进行牟利的僵尸网络。目前最新版本为3014。近日阿里云安全监控到来自此僵尸网络的攻击事件有增多趋势，攻击成功后，通过受控主机的crontab进行定期更新、运行。更新源：hxxp://149.56.106.215:8000/i.sh。

下载URL:

- hxxp://149.56.106.215:8000/i.sh
- hxxp://149.56.106.215:8000/static/3014/ddgs.i686
- hxxp://149.56.106.215:8000/static/3014/ddgs.x86_64

云防火墙可防御此类攻击，建议您开启云防火墙入侵防御能力。

恶意IP：149.56.106.215

事件：DDG蠕虫中控

威胁等级：高危

14.【基础规则】MySQL恶意UDF命令执行

MySQL提供用户自定义函数功能，这种由用户自行添加的MySQL函数就称为UDF（User Define Function）。但此过程经常被攻击者利用，当攻击者拿到MySQL的数据库权限后，就可以通过导入恶意库文件，进行自定义UDF，进而执行系统命令。

漏洞危害主要影响MySQL应用对外开放的应用服务器，存在高安全风险。可造成服务器被控制、数据泄漏、勒索、虚拟货币挖矿、对外DDoS等。

漏洞影响范围：MySQL 数据库

漏洞危险等级：高危

规则防护：云防火墙虚拟补丁已支持防护

规则类型：命令执行

15.【虚拟补丁】WebLogic任意文件上传漏洞（CVE-2018-2894）

阿里云云防火墙支持防护WebLogic任意文件上传漏洞。

WebLogic是由美国Oracle公司推出的application server，是基于JAVAEE架构的中间件。WebLogic是用于开发、集成、部署和管理大型分布式Web应用、网络应用和数据库应用的Java应用服务器。

ws_utc为WebLogic Web服务测试客户端，其配置页面存在未授权访问的问题，路径为/ws_utc/config.do。攻击者可通过访问此配置页面，用有效的WebLogic Web路径替换存储JKS Keystores的文件目录，然后上传恶意的JSP脚本木马文件。

影响范围：

- WebLogic 10.3.6.0
- WebLogic 12.1.3.0
- WebLogic 12.2.1.2
- WebLogic 12.2.1.3

漏洞危险等级：高危

规则防护：云防火墙虚拟补丁已支持防护

规则类型：命令执行

16.【威胁情报】Hadoop Yarn REST API未授权访问攻击

阿里云云防火墙可防护Hadoop Yarn REST API未授权访问攻击。

Hadoop是一款由Apache基金会推出的分布式系统框架，通过MapReduce算法进行分布式处理。Yarn是Hadoop集群的资源管理系统存在漏洞的主机，攻击者无需认证即可通过REST API部署任务来执行任意指令，最终完全控制服务器。

2018年10月25日阿里云监控到大量利用Hadoop Yarn REST API未授权访问漏洞的攻击事件。攻击成功后，受控主机会访问恶意源hxxps://bitbucket.org/*/raw/master/zz.sh下载恶意文件后进行挖矿。

漏洞危险等级：高危

规则防护：云防火墙虚拟补丁已支持防护

事件：Hadoop Yarn REST API未授权访问攻击