ALIBABA CLOUD

Alibaba Cloud

云防火墙
安全通告

文档版本：20200828

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.【虚拟补丁】Windows Server DNS Server远程代码执行（CVE-2020-1350）

2020年7月14日，阿里云应急响应中心监测到微软官方发布补丁修复了一个标注为远程代码执行的DNS Server漏洞（CVE-2020-1350），该漏洞被微软官方定义为“可蠕虫级”高危漏洞。

未经身份验证的攻击者可以利用此漏洞发送特殊构造的数据包到目标DNS Server，达到远程代码执行的效果。如果域控制器上存在DNS服务，攻击者可利用此漏洞获取到域控制器的系统权限。建议Windows用户尽快采取安全措施防止此漏洞攻击。

漏洞影响范围：

- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core)
- Windows Server 2012
- Windows Server 2012 (Server Core)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core)
- Windows Server 2016
- Windows Server 2016 (Server Core)
- Windows Server 2019
- Windows Server 2019 (Server Core)
- Windows Server, version 1903 (Server Core)
- Windows Server, version 1909 (Server Core)
- Windows Server, version 2004 (Server Core)

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

安全建议：

- 临时方案：修改*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters*中`TcpReceivePacketSize`的值为`0xFF00`，并重启DNS Service。
- 请您前往微软官方网站选择安全补丁进行更新。
- 使用云防火墙的入侵防御功能进行安全防护。

2.【虚拟补丁】Apache Dubbo反序列化代码执行（CVE-2020-1948）

2020年6月23日，阿里云应急响应中心监测到Apache Dubbo官方发布了Apache Dubbo远程代码执行的漏洞风险通告。

Apache Dubbo是一种基于Java的高性能RPC框架。Apache Dubbo官方披露在 `Dubbo Provider` 中存在一个反序列化远程代码执行漏洞（CVE-2020-1948），攻击者可以构造并发送带有恶意参数负载的RPC请求，当恶意参数被反序列化时将导致远程代码执行。

漏洞影响范围：

- Apache Dubbo 2.7.0~2.7.6
- Apache Dubbo 2.6.0~2.6.7
- Apache Dubbo 2.5.x系列所有版本（官方不再提供支持）

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

安全建议：

- Apache Dubbo官方已发布该漏洞的修复版本，请您升级至Apache Dubbo 2.7.7版本或更高版本。该漏洞修复版本的下载地址。
- 使用云防火墙的入侵防御功能进行安全防护。

3.【虚拟补丁】Windows SMBv3远程代码执行（CVE-2020-0796）

由于Microsoft Windows SMBv3协议中存在一处远程代码执行漏洞（漏洞CVE编号为CVE-2020-5405），微软安全中心在2020年3月12日23时发布了影响Windows系统的SMBv3远程代码执行漏洞的修复补丁。

该漏洞发生在 `srv2.sys` 中。由于SMBv3没有正确处理压缩的数据包，解压数据包时使用了客户端传输的长度进行解压，并没有检查长度是否合法，最终导致整数溢出。这种情况下，未经身份验证的远程攻击者可以通过构造恶意请求在Windows Server服务器上执行命令。

漏洞影响范围：

- Windows Server, version 1909（Server Core installation）
- Windows Server, version 1903（Server Core installation）
- Windows 10 Version 1903 for 32-bit Systems
- Windows 10 Version 1903 for x64-based Systems
- Windows 10 Version 1903 for ARM64-based Systems
- Windows 10 Version 1909 for 32-bit Systems
- Windows 10 Version 1909 for x64-based Systems
- Windows 10 Version 1909 for ARM64-based Systems

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

安全建议：

- 您可以安装修复补丁，具体请参见Windows官方说明。
- 使用云防火墙的入侵防御功能进行安全防护。

4.【基础规则】Oracle Coherence远程代码执行漏洞（CVE-2020-2555）

2020年3月6日，阿里云应急响应中心监测到Oracle Coherence反序列化远程代码执行漏洞（CVE编号：CVE-2020-2555）的细节已被公开。

Oracle Coherence是Oracle融合中间件中的产品，在WebLogic 12c及以上版本中默认集成到WebLogic安装包中。未经授权的攻击者可通过构造T3协议请求，绕过WebLoig的反序列化黑名单，从而通过反序列化代码执行命令控制WebLogic服务器。

云防火墙已监测到利用此漏洞发起的攻击，并且已支持拦截此类攻击。

漏洞影响范围：

- Oracle Coherence 3.7.1.17
- Oracle Coherence 12.1.3.0.0
- Oracle Coherence 12.2.1.3.0
- Oracle Coherence 12.2.1.4.0

漏洞危险等级：高危

规则防护：云防火墙基础规则已支持防护

规则类型：命令执行

安全建议：

- 进行版本升级或禁用WebLogic T3协议。
- 使用云防火墙的入侵防御功能进行安全防护。

5.【虚拟补丁】Apache Tomcat AJP协议文件读取与包含漏洞

Apache Tomcat是由Apache软件基金会下Jakarta项目开发的Servlet容器。默认情况下，Apache Tomcat会开启AJP连接器，方便与其他Web服务器通过AJP协议进行数据传输。

由于Apache Tomcat AJP协议的缺陷，攻击者通过Tomcat AJP Connector可以读取Apache Tomcat上所有*webapp*目录下的任意文件。攻击者读取*webapp*配置文件或源代码，在目标应用支持文件上传功能的情况下，配置文件中的应用还可以达到远程代码执行的危害。攻击者利用AJP服务端口的漏洞实行攻击，如果您未对外网开启AJP服务，则不受影响（Tomcat默认开启AJP服务并将其绑定至*0.0.0.0*）。

漏洞影响范围：Tomcat 6、7、8、9全版本默认配置下都会受到该漏洞影响

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

安全建议：

- 将Apache Tomcat版本升级到以下版本以上（包含以下版本）：
  - Apache Tomcat 7.0.100
  - Apache Tomcat 8.5.51
  - Apache Tomcat 9.0.31
- 使用云防火墙的入侵防御功能进行安全防护。

6.【威胁情报】Apache Dubbo反序列化漏洞（CVE-2019-17564）

2020年2月11日，阿里云应急响应中心监测到Apache Dubbo反序列化漏洞（CVE编号：CVE-2019-17564）。

Apache Dubbo是一款应用广泛的Java RPC分布式服务框架，支持多种协议，官方推荐使用Dubbo协议。Dubbo支持使用HTTP协议进行远程过程调用，该协议采用Spring HttpInvoker实现，在处理输入流时将会进行反序列化操作。当Apache Dubbo启用HTTP协议之后，Apache Dubbo在接受远程调用请求的时候存在一个不安全的反序列化行为，最终导致了远程任意代码执行。

云防火墙已监测到利用此漏洞发起的攻击，并支持拦截此类攻击。

漏洞影响范围：Apache Dubbo 2.7.5以下版本

漏洞危险等级：高危

安全建议：使用云防火墙的入侵防御功能进行安全防护。

7.【虚拟补丁】FusionAuth远程命令执行（CVE-2020-7799）

FusionAuth是一款访问管理开源应用程序，可以与多种技术和平台集成。您可以通过管理仪表板以多种方式配置和自定义FusionAuth，为任何应用程序提供身份验证、授权和用户管理。

FusionAuth 1.11之前版本，由于使用Apache FreeMarker模板引擎，且未对用户输入数据进行过滤。登录用户在进行电子邮件模板编辑时，可利用Apache FreeMarker模板引擎，调用freemarker.template.utility.Execute在底层操作系统上执行任意命令。

漏洞影响范围：FusionAuth 1.10.1版本及以下版本

漏洞危险等级：高危

规则防护：云防火墙基础规则已支持防护

规则类型：命令执行

安全建议：

- 升级FusionAuth版本到1.10.1以上。
- 使用云防火墙的入侵防御功能进行安全防护。

8.【基础规则】泛微E-cology OA系统远程代码执行漏洞

泛微OA产品E-cology是一款协同管理软件。阿里云云防火墙已支持防护泛微E-cology OA系统远程代码执行漏洞。

2019年9月19日，阿里云应急响应中心监测到泛微E-cology OA系统存在远程代码执行漏洞，即攻击者可通过构造特定的HTTP请求，获取目标服务器的操作权限，从而可未经授权进行远程执行命令。

漏洞出现原因：由于泛微E-cology OA系统自带BeanShell组件且开放未授权访问，导致攻击者可通过调用BeanShell组件接口直接在目标服务器上执行任意命令。

漏洞危险等级：高危

规则防护：云防火墙基础规则已支持防护

规则类型：命令执行

安全建议：

- 从官方渠道获取泛微E-cology OA安全升级方案。
- 使用云防火墙的入侵防御功能进行安全防护。

9.【虚拟补丁】Nexus Repository Manager 2.x远程命令执行（CVE-2019-5475）

Sonatype Nexus Repository Manager（NXRM）是美国Sonatype公司的一款Maven仓库管理器。

2019年9月6日，阿里云应急响应中心监测到Nexus Repository Manager 2.x版本存在远程命令执行漏洞，Nexus Repository Manager 2.x Capabilities可通过401认证登录，且可通过默认账号密码admin:admin123登录，登录成功后使用createrepo或mergerepo配置可实现远程系统命令注入。攻击者利用该漏洞可远程执行任意服务器命令，危害较大。

漏洞影响范围：Nexus Repository Manager OSS/Pro version 2.14.14以下版本

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

安全建议：升级Nexus Repository Manager 2.x至最新版本2.14.14。

10.【威胁情报】Windows RDP远程代码执行漏洞（CVE-2019-0708）

2019年9月6日，阿里云应急响应中心监测到安全工具metasploit释放了针对“BlueKeep（CVE-2019-0708）”的漏洞利用模块，阿里云已确认该利用程序可成功执行。利用此EXP代码，可以在目标系统上执行任意命令，甚至传播恶意蠕虫病毒感染内网其他机器。类似于2017年爆发的WannaCry等恶意勒索软件病毒，风险极高。

随着该漏洞利用程序的公开，漏洞利用门槛会大幅度降低，存在漏洞的主机极易被入侵。阿里云云防火墙提醒Windows相关用户注意漏洞资产排查，及时修复漏洞。

漏洞影响范围：

- Windows 7
- Windows Server 2008 R2
- Windows Server 2008
- Windows 2003
- Windows XP

漏洞危险等级：高危

安全建议：

- 及时对该漏洞进行修复。修复说明请参见微软安全公告。
- 使用云防火墙ACL对RDP协议进行限制（相关内容请参见访问控制策略总览），并建议仅放行白名单IP。

11.【虚拟补丁】Redis 4.x~5.x远程命令漏洞

2019年7月9日，阿里云应急响应中心监测到Redis存在远程命令执行漏洞。经过测试发现，Redis 4.0及5.0以上版本均受漏洞影响。漏洞产生的原因是在Reids 4.0版本之后Redis新增了模块功能，且在4.0以上版本默认支持。通过外部拓展，可以在Redis中实现一个新的Redis命令，并通过C语言编译出的*.so*文件执行系统命令，风险极高。

影响范围：Redis 4.0及5.0以上版本

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

安全建议：使用云防火墙的入侵防御功能进行安全防护。

12.【虚拟补丁】致远OA办公系统远程代码执行

2019年6月26日，阿里云应急响应中心监测到有社区媒体披露了致远OA办公系统远程代码执行漏洞。该漏洞是由于致远OA htmlofficeservlet HTTP接口在处理特定请求时存在缺陷，攻击者通过构造特定的HTTP请求，触发后可在目标服务器上执行任意命令。漏洞真实存在且风险极高。阿里云已捕获该0 day漏洞利用方式。

漏洞影响范围：致远OA办公系统

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

安全建议：

- 目前致远OA办公系统已发布官方安全补丁，您可从致远官方渠道获取安全补丁进行升级。
- 使用云防火墙的入侵防御功能进行安全防护。

13.【虚拟补丁】Windows RDP远程命令执行（CVE-2019-0708）

2019年5月15日，微软官方紧急发布安全补丁，修复了一个Windows远程桌面服务的远程代码执行漏洞(CVE-2019-0708)，该漏洞影响了某些旧版本的Windows系统。

该漏洞是预身份验证，无需用户交互。当未经身份验证的攻击者使用RDP（常见端口3389）连接到目标系统并发送特定请求时，可以在目标系统上执行任意命令，甚至传播恶意蠕虫病毒，感染内网其他机器。类似于2017年爆发的WannaCry等恶意勒索病毒。

漏洞影响范围：

- Windows 7
- Windows Server 2008 R2
- Windows Server 2008
- Windows 2003
- Windows XP

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

安全建议：

- 如果您是Windows 7、Windows Server 2008、Windows Server 2008 R2系统用户，请及时安装官方安全补丁。
- 如果您是Windows 2003、Windows XP系统用户，请及时更新系统版本或安装官网补丁。
- 使用云防火墙的入侵防御功能进行安全防护。
- 在云防火墙新增访问控制策略仅对RDP可信访问源放行或通过区域禁封功能仅对远程访问的常见区域放行，对其他未知访问或来自未知区域的连接尝试全部拒绝。

14.【虚拟补丁】WebLogic wls9-async反序列化远程命令执行

2019年4月17日，阿里云云盾应急响应中心监测到国家信息安全漏洞共享平台（CNVD）披露的“Oracle WebLogic wls9-async反序列化远程命令执行漏洞”。攻击者利用该漏洞可在未经授权的情况下远程执行命令。

WebLogic部分版本中默认包含的wls9_async_response包，为WebLogic Server提供异步通讯服务。由于该War包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，获得目标服务器的权限，在未经授权的情况下远程执行命令。

漏洞影响范围：Oracle WebLogic 10.X和Oracle WebLogic 12.1.3

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

15.【威胁情报】MongoDB数据库未授权访问漏洞

MongoDB数据库未授权访问漏洞危害严重，可能导致数据库数据泄露或被删除勒索，从而造成严重的生产事故。

2019年2月14日，国家互联网应急中心CNCERT监测发现，我国境内部分MongoDB数据库暴露在互联网上导致重要信息泄露。

漏洞危害：

MongoDB服务启动时，如果不修改数据库认证访问权限相关的默认配置，登录的用户无需权限验证即可通过默认端口（无需密码）本地或远程访问该数据库，并对数据库进行任意操作（增、删、改、查等高危操作）。

为保证您的业务和应用的安全，请参见MongoDB数据库未授权访问漏洞防御最佳实践尽快修复该漏洞。

16.【虚拟补丁】Confluence远程文件读取漏洞（CVE-2019-3396）

Confluence是一个专业的企业知识管理与协同软件，可用于构建企业wiki。

2019年4月4日，阿里云安全应急响应中心监测到Confluence官方发布安全更新，Widget Connector存在服务端模板注入漏洞，攻击者能利用此漏洞实现目录穿越遍历甚至远程命令执行。

近期阿里云安全应急响应中心监测到最新的漏洞利用方式流出，且多款蠕虫开始利用此漏洞进行传播。

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

安全版本：

- Version 6.6.12 and higher versions of 6.6.x
- Version 6.12.3 and higher versions of 6.12.x
- Version 6.13.3 and higher versions of 6.13.x
- Version 6.14.2 and higher

17.【威胁情报】Jenkins攻击预警

2019年2月28日，阿里云安全监控到针对Jenkins漏洞的攻击利用方式在网上披露较多，且多为远程代码执行的高危漏洞。另有多种蠕虫的传播方式添加了Jenkins远程代码执行漏洞，危害极大。

目前监测到使用较多的漏洞CVE编号为：CVE-2019-1003000、CVE-2019-1003001、CVE-2015-5323、CVE-2015-1814、CVE-2016-0792、CVE-2017-1000353，且漏洞涉及多个Jenkins版本和插件。

漏洞危险等级：高危

阿里云云防火墙可在漏洞攻击、蠕虫植入、恶意文件下载等阶段对此攻击进行多维度防御。建议开启阿里云云防火墙入侵防御能力。

18.【虚拟补丁】Nexus Repository Manager 3远程代码执行（CVE-2019-7238）

Nexus Repository Manager（简称NXRM）是由Sonatype公司研发的一款通用的软件包仓库管理服务，可以作为Maven的私服。

部分版本的Nexus Repository Manager存在安全漏洞，受漏洞影响的软件版本存在控制措施缺失，未授权的用户可利用该缺陷构造特定请求在服务器上执行Java代码，从而达到远程代码执行的目的，影响系统安全。

漏洞描述请参见：CVE-2019-7238 Nexus Repository Manager 3 (Missing Access Controls and Remote Code Execution) - February 5th 2019

漏洞影响范围：Nexus Repository Manager OSS/Pro 3.6.2~3.14.0版本

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

19.【基础规则】Jenkins远程代码执行（CVE-2019-1003000）

Jenkins是一个开源软件项目，是基于Java开发的一种持续集成工具。Script Security and Pipeline插件是Jenkins的一个安全插件，可以集成到Jenkins各种功能插件中。

近日，阿里云应急响应中心监控到Jenkins的Script Security and Pipeline插件远程代码执行漏洞（CVE编号：CVE-2019-1003000）的利用方式在互联网上被公布。拥有Overall/Read权限的用户可以绕过沙盒保护，在jenkins上执行任意代码，危害极大。

漏洞描述请参见：Jenkins Security Advisory 2019-01-08。

漏洞影响范围：

- Declarative Plugin 1.3.4.1版本以下
- Groovy Plugin 2.61.1版本以下
- Script Security Plugin 1.5.0版本以下

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

20.【虚拟补丁】Kubernetes用户权限提升（CVE-2018-1002105）

Kubernetes（简称K8s），是用8代替8个字符“ubernete”而成的缩写。K8s是一个开源的、用于管理云平台中多个主机上的容器化的应用。

通过伪造请求，K8s普通用户可以在已建立的API Server连接上提升访问后端服务的权限，实现提升从K8s普通用户到K8s API server的权限。这里的普通用户至少需要有一个pod的exec/attach/portforward等权限。连接建立后，攻击者就可以通过网络连接直接向后端服务发送任意请求，实现对K8s集群中所有节点机器的所有控制操作，包括ROOT权限。

部署受影响版本的服务器存在高危入侵风险，建议开启云防火墙进行拦截，具体请参见入侵防御能力。

漏洞影响范围：

- Kubernetes v1.0.x~1.9.x
- Kubernetes v1.10.0~1.10.10 (fixed in v1.10.11)
- Kubernetes v1.11.0~1.11.4 (fixed in v1.11.5)
- Kubernetes v1.12.0~1.12.2 (fixed in v1.12.3)

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

21.【基础规则】ThinkPHP 5.1~5.2多个版本远程代码执行

2019年1月15日，阿里云应急响应中心监测到ThinkPHP 5.1~5.2版本在一定条件下存在远程代码执行漏洞。

此漏洞是由于ThinkPHP 5.0框架对Request类的method处理存在缺陷，导致黑客构造特定的请求，可直接获取Webshell。

近两个月，ThinkPHP5框架连续披露多个可远程执行命令的高危漏洞。云防火墙已上线针对此漏洞的防护规则，对攻击行为进行实时监控和拦截。

漏洞影响范围： ThinkPHP V5.1 ~ V5.2

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

22.【基础规则】ThinkPHP 5.0.24以下版本远程代码执行

ThinkPHP是源自中国的一个快速、兼容而且简单的轻量级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。

2019年1月11日，ThinkPHP官方发布安全更新，披露了一个高危安全漏洞：攻击者构造特定的恶意请求，可以直接获取服务器权限。

此漏洞是由于ThinkPHP 5.0框架对Request类的method处理存在缺陷，导致攻击者构造特定的请求，可直接获取Webshell。

漏洞影响范围：ThinkPHP V5.0.0~5.0.24

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

23.【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

24.【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

25.【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

26.【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

27.【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

28.【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

29.【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

30.【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

31.【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

32.【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

33.【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QBotVariant。QBotVariant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。QBotVariant可在互联网上广泛传播并造成极大的危害。

QBotVariant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

34.【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

35.【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

36.【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

37.【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