Web 应用防火墙

动态与公告

产品文档

腾讯云

文档目录

动态与公告

产品动态

最近更新时间：2022-06-23 11:14:26

2022-06

动态名称	动态描述	发布时间	相关文档
体验升级	优化非中国大陆 Web 应用防火墙实例数据存储，支持不同地区资源数据隔离查看，提升用户操作和管理体验。	2022-06-03	-
操作日志	支持控制台内查看云审计内的 Web 应用防火墙的操作日志，支持用户操作查询和溯源。	2022-06-03	-
实例列表	支持用户购买多版本或者升级跨版本 Web 应用防火墙实例，满足用户根据自身业务需求选择不同版本的实例防护需求。	2022-06-03	-
接入模式	回源模式，支持用户自定义配置多 IP 加权轮询权限，满足复杂业务SAAS化接入的负载均衡需求。	2022-06-03	-
IP 封禁能力增强	支持基于域名的 IP 封禁能力，防护更精细。	2022-06-03	-
区域封禁	支持用户一键配置区域封禁功能，提升访问控制配置体验。	2022-06-03	-
一键开关防护	支持一键开启和关闭全部防护模块，以及部分防护功能模块的防护能力，助力用户快速处置日常运维过程中的业务问题排查，虽缩短定位周期，保障业务连续性。	2022-06-03	-
精细化流量管理	升级 IP 黑白名单为黑白名单管理，将原来自定义策略中处置动作为“放行”的规则升级为精准白名单规则，其他自定义策略规则升级为访问控制规则。规则本身的配置和执行效果不受升级影响。 通过精准白名单，支持用户日常安全运维的精细化流量管理，提升用户业务流量管控效率和效果，保证用户业务的安全性。	2022-06-03	-
日志服务	用户升级购买日志服务增值服务后，支持自主开启实时存储全量访问日志存储和查询。	2022-06-03	-
自定义流量标记	支持用户自定义流量标记能力，满足复杂的用户业务	2022-06-03	-

	分析和联动防护诉求。		
域名接入向导支持	新增域名接入配置向导，完善域名添加后续步骤引导，贴心守护接入过程，业务接入更轻松。	2022-06-03	-
BOT 防护全面防护	BOT 防护全面升级，支持前端对抗、威胁情报、以及智能 AI 评估能力，通过综合打分精准识别 BOT 流量，增加可视化流量分析功能。	2022-06-03	-
BOT 报表	快速的发现当前网站面临的 BOT 风险，快速得知哪些接口正在遭受 BOT 风险，快速定位 BOT 关注资源，并能快速制定针对性的 BOT 对抗策略，保障网站业务安全。	2022-06-03	-

产品公告
关于 Web 应用防火墙-BOT流量管理计费方式调整公告

最近更新时间：2023-09-08 18:23:10

为了给BOT流量管理功能的用户提供更优质的服务，腾讯云 Web 应用防火墙（Web Application Firewall，简称 WAF）计划于2023年10月11日 调整BOT流量管理的计费方式。

具体调整如下：

调整前， BOT流量管理为单独计费，支持防护的QPS上限为2500QPS/月，超出上限支持购买预付费BOT业务拓展包、单价为750美元/1000QPS/月。

调整后，BOT流量管理和WAF的 QPS规格合并计费，购买BOT流量管理后支持防护的BOT流量峰值与WAF主版本QPS默认防护规格一致；同时BOT流量管理的业务拓展包将停止新购，BOT流量管理QPS超出上限后支持购买WAF预付费主版本业务拓展包进行扩展。如用户已经购买了WAF业务拓展包且开通了BOT流量管理，那么在扩展BOT流量管理防护时，中国大陆扩展包增购单价仅为275美元/1000QPS/月，非中国大陆扩展包增购单价仅为300美元/1000QPS/月。

以上策略将于2023年09月起陆续灰度并于2023年10月11日正式执行。感谢您的关注和支持，如对计费调整存在疑问，请随时与我们联系。

Web 应用防火墙发布公告

最近更新时间：2022-09-16 18:06:02

国际站发布动态公告

为提升非中国大陆地区的业务接入和防护能力配置体验，2022年6月2日， Web应用防火墙的产品能力全新升级，并上线Web2.0版本控制台。升级后，接入更稳定，防护能力更强大、流量管理支持更精细，并支持BOT 流量管理和日志服务的增值能力；同时，控制台将增加中国大陆和非中国大陆地区划分，并支持通过地区切换控制切换，管理不同地区的实例资源。

具体对不同类型的WAF实例影响如下：

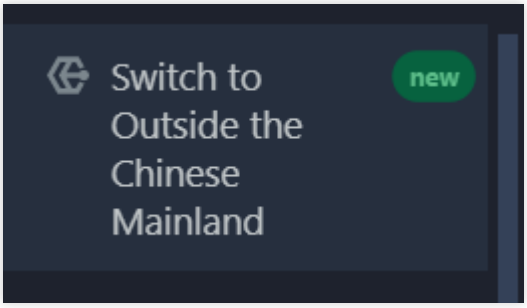
SAAS型WAF实例，WAF继续保持实例地域属性，系统自动根据地域字段增加地区字段，产品控制台区分地区管理，其他无变化。

负载均衡型WAF：中国大陆地区的WAF实例仅支持中国大陆CLB实例的web业务接入防护；非中国大陆地区的WAF实例仅支持非中国大陆CLB实例的web业务接入防护。

本次 Web2.0升级后，您将获得以下产品能力和配置体验：

支持跨地区资源数据隔离

控制台将增加中国大陆和非中国大陆地区划分，并支持通过地区切换控制切换，详细如下图，支持在控制台菜单进行切换：



域名接入全面升级、更快捷

域名接入和管理能力升级

支持多实例统一管理，助力用户提升日常安全运维效率。SAAS型WAF，IP回源支持用户自定义加权回源，满足复杂业务接入需求；域名回源支持多域名回源配置。

域名接入向导支持

新增域名接入配置向导，完善域名添加后续步骤引导，贴心守护接入过程，业务接入更轻松。

自定义流量标记

SAAS型WAF接入支持用户自定义流量标记能力，满足复杂的用户业务分析和联动防护诉求。

客户端信息记录

SAAS型WAF支持用户自定义配置开启传递业务客户端的源 IP 地址和端口信息，补充 XFF 记录内容，助力金融、电商等行业客户业务监管合规。

防护能力升级

一键开关防护

支持一键开启和关闭全部防护模块，以及部分防护功能模块的防护能力，助力用户快速处置日常运维过程中的业务问题排查，虽缩短定位周期，保障业务连续性。

精细化流量管理

升级 IP 黑白名单为黑白名单管理，将原来自定义策略中处置动作为“放行”的规则升级为精准白名单规则，其他自定义策略规则升级为访问控制规则。规则本身的配置和执行效果不受升级影响。
通过精准白名单，支持用户日常安全运维的精细化流量管理，提升用户业务流量管控效率和效果，保证用户业务的安全性。

产品增值能力升级--BOT 流量管理商业化发布

全新 BOT 一体化防护系统，联合前端对抗、威胁情报、以及大数据 AI 算法模型分析引擎三大防线，为用户提供基于风险度的流量可视化分析，构造威胁处置策略更加直观。

安全公告

Apache log4j2 远程代码执行漏洞风险公告（CVE-2021-44832）

最近更新时间：2022-06-23 11:14:26

2021年12月29日，腾讯云安全运营中心监测到，**Apache Log4j2 官方发布公告提示其在某些特殊场景下存在远程代码执行漏洞，漏洞编号 CVE-2021-44832。该漏洞仅在攻击者拥有修改配置文件权限时才可远程执行任意代码，漏洞利用难度较大。**

为避免您的业务受影响，腾讯云安全建议您及时开展安全自查，如在受影响范围，请您及时进行更新修复，避免被外部攻击者入侵。

漏洞详情

Apache Log4j2 是一个基于 Java 的开源日志记录框架，该框架重写了 Log4j 框架，是其前身 Log4j 1.x 的重写升级版，并且引入了大量丰富的特性，使用非常的广泛。该框架被大量用于业务系统开发，用来记录日志信息。

据官方描述，拥有修改日志配置文件权限的攻击者，可以构造恶意的配置将 JDBC Appender 与引用 JNDI URI 的数据源一起使用，从而可通过该 JNDI URI 远程执行任意代码。

由于该漏洞要求攻击者拥有修改配置文件权限（通常需借助其他漏洞才可实现），非默认配置存在的问题，漏洞成功利用难度较大。

风险等级

中风险。

漏洞风险

可导致攻击者利用该漏洞远程执行任意代码。

影响版本

2.0-beta7 =< Apache Log4j 2.x < 2.17.0（2.3.2 和 2.12.4 版本不受影响）

安全版本

- Apache Log4j 2.x >= 2.3.2 (Java 6)
- Apache Log4j 2.x >= 2.12.4 (Java 7)
- Apache Log4j 2.x >= 2.17.1 (Java 8 及更新版)

修复建议

目前 Apache Log4j2 官方已有可更新版本，用户可以参照 官方说明 酌情升级至安全版本。

> 注意：
> 建议您在升级前做好数据备份工作，避免出现意外。

腾讯安全解决方案

腾讯云 高级威胁检测系统 规则库日期2021-12-29之后的版本，已支持检测 log4j2 远程代码执行漏洞（CVE-2021-44832）。

参考信息

更多信息，请参见 官方安全更新公告 。

Apache Log4j 2 远程代码执行漏洞风险公告（CVE-2021-45046）

最近更新时间：2022-06-23 11:14:26

2021年12月17日，腾讯云安全运营中心监测到，**Apache Log4j 由于非默认配置下对CVE-2021-44228修复措施不完善，导致在某些特殊配置场景下，可被攻击者利用造成远程代码执行攻击。**

为避免您的业务受影响，腾讯云安全建议您及时开展安全自查，如在受影响范围，请您及时进行更新修复，避免被外部攻击者入侵。

漏洞详情

Apache Log4j 2 是一个开源的日志记录组件，是 Apache Log4j 的升级版，它可以控制每一条日志的输出格式，通过定义每一条日志信息的级别，能够更加细致地控制日志的生成过程。

继2021年12月9日被曝存在严重代码执行漏洞（CVE-2021-44228）后，**Apache Log4j 官方近日又披露了另外一个远程执行漏洞（CVE-2021-45046），漏洞风险已从之前的 CVSS 3.7分上升到 CVSS 9.0分，该漏洞与非默认配置下对 CVE-2021-44228修复措施不完善有关，在线程上下文查找模式的某些非默认配置中，攻击者可以构造特定请求，实现远程代码执行。**

该漏洞也同时影响全球大量通用应用及组件，例如 ：
Apache Struts2
Apache Solr
Apache Druid
Apache Flink
Apache Dubbo
Apache Kafka
Spring-boot-starter-log4j2
ElasticSearch
Logstash
...
建议及时检查并升级所有使用了 Log4j 组件的系统或应用。

风险等级

高风险（CVSS 评分：9.0）。

漏洞风险

可导致攻击者利用该漏洞远程执行任意代码。

影响版本

2.0-beta9 =< Apache Log4j 2.x < 2.16.0（2.12.2 版本不受影响）

安全版本

- Apache log4j 2.16.0 （Java 8）
- Apache Log4j 2.12.2（Java 7）

修复建议

建议开展内部自查，检查业务应用是否引入了 Apache log4j-core Jar 包，若存在依赖引入，且在受影响版本范围内，则可能存在漏洞影响，可采取如下措施：

> 注意：
> 建议您在升级前做好数据备份工作，避免出现意外。

升级到官方最新版本（推荐）

目前官方已发布修复版本，用户可以根据自身情况升级或者将代码更新到该版本

- Java 8 用户：需升级到 Apache Log4j 2.16.0版本。
- Java 7 用户：需升级到 Apache Log4j 2.12.2版本。

应用其他防护方案

1. 对于暂时无法升级版本的用户，建议移除 log4j-core 包中 JndiLookup 类文件，并重启服务，可用以下命令：

```
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

2. 通过安全组或防火墙限制受影响应用对外访问互联网。

参考信息

更多信息，请参见 官方安全更新公告 。

Apache Log4j 2 远程代码执行漏洞风险公告（CVE-2021-44228）

最近更新时间：2022-06-23 11:14:26

2021年12月09日，腾讯云安全运营中心监测到，**Apache Log4j 2 被披露出存在严重代码执行漏洞，目前官方已发布正式安全公告及版本（漏洞编号：CVE-2021-44228），漏洞被利用可导致服务器被入侵等危害。**

为避免您的业务受影响，腾讯云安全建议您及时开展安全自查，如在受影响范围，请您及时进行更新修复，避免被外部攻击者入侵。

漏洞详情

Apache Log4j 2是一个开源的日志记录组件，使用非常的广泛。在工程中以易用方便代替了 System.out 等打印语句，它是 Java 下最流行的日志输入工具。

使用 Log4j 2 在一定场景条件下处理恶意数据时，可能会造成注入类代码执行。

由于Log4j2 作为日志记录基础第三方库，被大量 Java 框架及应用使用，只要用到 Log4j2 进行日志输出且日志内容能被攻击者部分可控，即可能会受到漏洞攻击影响。因此，该漏洞也同时影响全球大量通用应用及组件，例如 ：
Apache Struts2
Apache Solr
Apache Druid
Apache Flink
Apache Flume
Apache Dubbo
Apache Kafka
Spring-boot-starter-log4j2
ElasticSearch
Logstash
...
建议及时检查并升级所有使用了 Log4j 组件的系统或应用。

风险等级

高风险。

漏洞风险

可导致攻击者利用该漏洞远程执行任意代码。

影响版本

Apache log4j2 >= 2.0, <= 2.14.1

安全版本

Apache log4j2 2.16.0

修复建议

升级到官方最新版本（推荐）

目前官方最新版本为 log4j-core-2.16.0，用户可以升级或者将代码更新到该版本。

关闭 log4j 的 lookup 功能

配置文件方式关闭（推荐）

在应用程序的 classpath 中的 log4j2.component.properties 配置文件（如果没有文件，则手工新建）中添加如下两行内容（>=2.9.1以及之后版本）。

```
log4j2.formatMsgNoLookups=True
log4j.formatMsgNoLookups=True
```

jvm 参数配置关闭（不推荐，容易丢失配置）

在 JVM 启动参数中加上 `-Dlog4j2.formatMsgNoLookups=true` 和 `-Dlog4j.formatMsgNoLookups=true` 。

> 说明：
> 对于2.0~2.10版本，应先升级至2.10+，再增加 jvm 参数。

升级到高版本 JDK（推荐）

高版本 JDK 有一些安全限制，建议升级 JDK 到6u211、7u201、8u191、11.0.1及以上的版本，可以在一定程度上限制 JNDI 等漏洞利用方式。

其他临时缓解措施

禁止不必要的业务访问外网，可通过防火墙、安全组等，禁止相关应用及业务主动对外连接。

腾讯安全解决方案

腾讯云 Web 应用防火墙已支持检测拦截利用 Log4j2 远程代码执行漏洞的攻击活动。

参考信息

更多信息，请参见 官方安全更新公告。

Weblogic Console HTTP 协议远程代码执行漏洞公告

最近更新时间：2022-06-23 11:14:26

漏洞详情

2020年10月20日，腾讯安全团队检测到 Oracle 发布的 安全更新公告 。在本次更新的 Weblogic 相关漏洞中的 CVE-2020-14882 及 CVE-2020-14883 漏洞，存在于 WebLogic 的 Console 控制台中。此组件为 WebLogic 全版本默认自带组件，攻击者通过将 CVE-2020-14882 和 CVE-2020-14883 漏洞进行组合利用后，在未经授权的情况下，可以直接在服务端执行任意代码，获取系统权限，控制 Oracle WebLogic Server，影响数据的保密性、完整性和可用性。
腾讯安全旗下的全系列安全产品已针对该漏洞升级规则库及漏洞库，以防御黑客攻击利用。
为避免您的业务受影响，腾讯云安全建议您及时开展安全自查，如在受影响范围，请您及时进行更新修复，避免被外部攻击者入侵。

风险等级

高风险。

漏洞风险

攻击者可利用该漏洞控制 Oracle WebLogic Server，影响数据的保密性、完整性和可用性。

影响版本

Oracle Weblogic Server 10.3.6.0.0
Oracle Weblogic Server 12.1.3.0.0
Oracle Weblogic Server 12.2.1.3.0
Oracle Weblogic Server 12.2.1.4.0
Oracle Weblogic Server 14.1.1.0.0

修复建议

官方已发布新版本安全产品修复该漏洞，腾讯云安全建议您：

推荐方案：及时 安装更新补丁。

使用 Web 应用防火墙拦截防御此类 Weblogic 漏洞攻击。

参考信息

更多信息，请参见 官方安全更新公告 。

Exchange Server 命令执行漏洞的安全防护公告

最近更新时间：2022-06-23 11:14:26

2020年9月17日，腾讯安全团队检测到 Microsoft 发布了 Exchange Server 命令执行漏洞的安全公告，该漏洞编号为 CVE-2020-16875。

说明：

Microsoft Exchange Server 是美国微软（Microsoft）公司的一套电子邮件服务程序，它提供邮件存取、储存、转发、语音邮件及邮件过滤筛选等功能。

目前该漏洞 POC 已经在网络上流传，腾讯安全团队建议及时将 Exchange 升级到最新版本，做好资产自查以及相关防护工作，以免遭受黑客恶意攻击。目前腾讯云 Web 应用防火墙已支持防御。

漏洞详情

Microsoft Exchange 服务器中存在一个远程执行代码漏洞。此次漏洞是由于 Exchange 对 cmdlet 参数的验证不全面，使攻击者成功利用此漏洞在系统用户的上下文中运行任意代码。此漏洞需要通过 Exchange 身份验证才能利用。由于 Exchange 服务以 SYSTEM 权限运行，攻击者可通过利用该漏洞获得系统最高权限。

影响版本

Microsoft Exchange Server 2016 Cumulative Update 16
Microsoft Exchange Server 2016 Cumulative Update 17
Microsoft Exchange Server 2019 Cumulative Update 5
Microsoft Exchange Server 2019 Cumulative Update 6

修复建议

根据漏洞通告信息，腾讯安全建议您：
及时更新漏洞补丁。
推荐采取腾讯云 Web 应用防火墙检测并防御此次攻击。

参考信息

CVE-2020-16875

用友 GRP-U8 行政事业内控管理软件存在 SQL 注入漏洞公告

最近更新时间：2022-06-23 11:14:26

2020年9月11日，腾讯安全团队检测到用友 GRP-U8 行政事业内控管理软件存在 SQL 注入漏洞，攻击者可通过精心构造的 payload 进行 SQL 注入攻击，从而获取数据库敏感信息。
目前已发现在野利用，腾讯云 Web 应用防火墙已支持防御。

漏洞详情

攻击者通过精心构造的 payload 进行 SQL 注入攻击从而获取数据库敏感信息，目前腾讯云 Web 应用防火墙已支持防御。

影响版本

用友 GRP-U8 行政事业内控管理软件。

修复建议

根据漏洞通告信息，目前官方尚无更新信息，腾讯安全建议您：
由于软件的敏感性，建议不开放在公网，或使用白名单策略。
推荐采取腾讯云 Web 应用防火墙检测并拦截此次攻击。

参考信息

CNVD-2020-49261
用友政务官方网站

CVE-2020-11991 Apache Cocoon XML 外部实体注入漏洞公告

最近更新时间：2022-06-23 11:14:26

2020年9月11日，Apache 软件基金会发布安全公告，修复了 Apache Cocoon XML 外部实体注入漏洞（CVE-2020-11991）。

漏洞详情

Apache Cocoon 是一个基于 Spring 框架，围绕分离理念建立的构架，在该框架下的所有处理都被预先定义好的处理组件线性连接起来，能够将输入和产生的输出按照流水线顺序处理。用户群包括 Apache Lenya、Daisy CMS、Hippo CMS、Mindquarry 等等，Apache Cocoon 通常被作为一个数据抽取、转换、加载工具或系统之间传输数据的中转站。
CVE-2020-11991 与 StreamGenerator 有关，Cocoon 在使用 StreamGenerator 时，将解析用户提供的 XML。攻击者通过包括外部系统实体在内的特制 XML 来访问服务器系统上的任何文件。

风险等级

高风险

漏洞风险

攻击者可以通过包括外部系统实体在内的特制 XML 来访问服务器系统上的任何文件。

影响版本

Apache Cocoon <= 2.1.12

修复建议

目前厂商已在新版本修复该漏洞，腾讯安全建议您：
用户应升级到 Apache Cocoon 2.1.13 最新版本

腾讯云 Web 应用防火墙（Web Application Firewall）已支持拦截防御 CVE-2020-11991 此类 XXE 漏洞。

注意：

建议您在安装补丁前做好数据备份工作，避免出现意外。

参考信息

官方更新通告：

Apache Cocoon

Apache Cocoon 2.2

CVE-2020-11991

WordPress File Manager 存在任意代码执行漏洞公告

最近更新时间：2022-06-23 11:14:27

2020年9月6日，腾讯安全团队检测到 WordPress 插件 File Manager 存在任意代码执行漏洞，攻击者利用该漏洞可以在含有 File Manager 的 WordPress 网站中上传木马、执行任意命令和恶意脚本。
腾讯安全已捕获在野利用（现网利用），目前腾讯云 Web 应用防火墙已支持防御。

漏洞详情

腾讯安全团队检测到 WordPress 插件 File Manager 被曝存在任意代码执行漏洞，攻击者利用该漏洞可以在含有 File Manager 的 WordPress 网站中上传木马、执行任意命令和恶意脚本。在 wordpress.org 的插件库中， File Manager 在2020年9月1日之前提供的 v6.8 版本为受影响版本，可以被攻击者用于破坏网站。
默认情况下，无需认证可以直接打开文件 lib/php/*.php ，并且该文件加载 lib/php/*.php，该文件读取 POST/GET 变量，并允许执行一些内部功能，例如上传文件等，由于允许使用 PHP 代码，因此会导致未经身份验证的任意文件上传和远程代码执行。

影响版本

WordPress File Manager < 6.9

修复建议

官方发布升级插件修复该漏洞，腾讯安全建议您：
更新 WordPress File Manager 版本至6.9及以上。
推荐采取腾讯云 Web 应用防火墙检测并拦截此次攻击。

参考信息

CVE 2020-25213

Jenkins 发布9月安全更新公告

最近更新时间：2022-06-23 11:14:27

2020年9月3日，腾讯安全团队监控到 Jenkins 发布了9月安全通告，里面包含14个 CVE 漏洞（CVE-2020-2238，CVE-2020-2239，CVE-2020-2240， CVE-2020-2241， CVE-2020-2242， CVE-2020-2243， CVE-2020-2244，CVE-2020-2245， CVE-2020-2246， CVE-2020-2247， CVE-2020-2248， CVE-2020-2249， CVE-2020-2250，CVE-2020-2251），有10个插件受影响，涉及以下插件：

Build Failure Analyzer Plugin

Cadence vManager Plugin

database Plugin

Git Parameter Plugin

JSGames Plugin

Klocwork Analysis Plugin

Parameterized Remote Trigger Plugin

SoapUI Pro Functional Testing Plugin

Team Foundation Server Plugin

Valgrind Plugin

其中以下漏洞定义为高危：

CVE-2020-2248（JSGames Plugin XSS 漏洞）

CVE-2020-2247（Klocwork Analysis Plugin 中的 XXE 漏洞）

CVE-2020-2246（Valgrind plugin XSS 漏洞）

CVE-2020-2245（Valgrind plugin XXE 漏洞）

CVE-2020-2244（Build Failure Analyzer Plugin 存在 XSS 漏洞）

CVE-2020-2243（Cadence vManager Plugin 存在存储型 XSS 漏洞）

CVE-2020-2240（database Plugin CSRF 漏洞）

CVE-2020-2238（Git Parameter Plugin 存储型 XSS 漏洞）

Jenkins 是一款基于 Java 开发的开源项目，用于持续集成和持续交付的自动化中间件，是开发过程中常用的产品，为避免您的业务受影响，腾讯云安全建议您及时开展安全自查，如在受影响范围，请您及时进行更新修复，避免被外部攻击者入侵。由于有部分漏洞目前尚无修补程序，建议使用采取腾讯 Web 应用防火墙进行防御。

漏洞详情

Git Parameter Plugin 存在存储型 XSS 漏洞 （CVE-2020-2238）

Git Parameter Plugin 0.9.12 及更早版本不会在“Build with Parameters”页面上转义，导致存储的跨站点脚本（XSS）漏洞可由具有“Job/Configure”权限的攻击者利用。

Git Parameter Plugin 在0.9.13上完成修复工作。

Parameterized Remote Trigger Plugin 将密码明文存储在纯文本中（CVE-2020-2239）。

Parameterized Remote Trigger Plugin 3.1.3和更早版本将密码明文存储。

database Plugin 存在 CSRF 漏洞 CVE-2020-2240

database Plugin 1.6 和更早版本不需要数据库控制台的 POST 请求，从而导致跨站点请求伪造（CSRF）漏洞，此漏洞使攻击者可以执行任意 SQL 脚本。

database Plugin CSRF 漏洞和越权漏洞 CVE-2020-2241 (CSRF)，CVE-2020-2242（permission check）。

database Plugin 1.6 和更早版本在实现表单验证的方法中不执行权限检查。 这使具有对 Jenkins 的“Overall/Read ”访问权限的攻击者，可以使用攻击者指定的用户名和密码连接到攻击者指定的数据库服务器。此外，此表单验证方法不需要 POST 请求，从而导致跨站点请求伪造（CSRF）漏洞。

database Plugin 1.7 需要 POST 请求和受影响的表单验证方法的“Overall/Read”权限。

Cadence vManager Plugin 存在存储型 XSS 漏洞 CVE-2020-2243

Cadence vManager Plugin 3.0.4 及更早版本不会在工具提示中转义构建说明，从而导致存储的跨站点脚本（XSS）漏洞可由具有运行/更新权限的攻击者利用。

Cadence vManager Plugin 3.0.5 删除了受影响的工具提示。

Build Failure Analyzer Plugin 存在 XSS 漏洞 CVE-2020-2244

Build Failure Analyzer Plugin 1.27.0 及更早版本不会在表单验证响应中转义匹配的文本，从而导致跨站点脚本（XSS）漏洞，攻击者可以利用此漏洞，为用于测试构建日志指示的构建提供控制台输出。

Build Failure Analyzer Plugin 1.27.1 会在受影响的表单验证响应中转义匹配的文本。

Valgrind Plugin 存在 XXE 漏洞 CVE-2020-2245

Valgrind Plugin 0.28 和更早版本没有配置其 XML 解析器来防止 XML 外部实体（XXE）攻击，从而使攻击者能够控制 Valgrind Plugin 解析器的输入文件，使 Jenkins 解析使用外部实体，从 Jenkins 控制器或服务器端请求伪造中提取机密的制作好的文件。

截至本公告发布之时，尚无修复程序。

Valgrind Plugin 中存储的 XSS 漏洞 CVE-2020-2246

Valgrind Plugin 0.28 和更早版本不会在 Valgrind XML 报表中转义内容，从而导致存储的跨站点脚本（XSS）漏洞可由能够控制 Valgrind XML 报告内容的攻击者利用。

截至本公告发布之时，尚无修复程序。

Klocwork Analysis Plugin 中的 XXE 漏洞 CVE-2020-2247

Klocwork Analysis Plugin 2020.2.1和更早版本没有配置其 XML 解析器来防止 XML 外部实体（XXE）攻击，从而攻击者能够控制 Klocwork 插件解析器的输入文件，使 Jenkins 解析使用外部实体，从 Jenkins 控制器或服务器端请求伪造中提取机密的制作好的文件。

截至本公告发布之时，尚无修复程序。

JSGames Plugin 存在反射型的 XSS 漏洞 CVE-2020-2248

JSGames Plugin 0.2及更早版本将 URL 的一部分作为代码进行评估，从而会导致反映出跨站点脚本（XSS）漏洞。

截至本公告发布之时，尚无修复程序。

Team Foundation Server Plugin 以明文格式存储凭据 CVE-2020-2249

Team Foundation Server Plugin 5.157.1 和更早版本将 Webhook 机密未加密地存储，在 Jenkins 控制器的全局配置

文件中 hudson.plugins.tfs.TeamPluginGlobalConfig.xml 作为其配置的一部分，攻击者可以访问 Jenkins 控制器文件系统来查看此凭据。

SoapUI Pro Functional Testing Plugin 使用明文存储密码 CVE-2020-2250

SoapUI Pro Functional Testing Plugin 1.3 和更早版本将未加密的项目密码存储在 job config.xml 文件中，作为其配置的一部分，具有扩展读取权限或访问 Jenkins 控制器文件系统的攻击者可以查看这些项目密码。一旦再次保存受影响的 job 配置，SoapUI Pro Functional Testing Plugin 1.4 将存储加密的项目密码。

SoapUI Pro Functional Testing Plugin 使用明文传输密码 CVE-2020-2251

SoapUI Pro 功能测试插件将项目密码存储在 Jenkins 控制器上的 job 文件中，config.xml 作为其配置的一部分。

自 SoapUI Pro 功能测试插件1.4起，这些密码以加密方式存储在磁盘上，但 SoapUI Pro 功能测试插件1.5及更早版本以全局配置形式将它们以纯文本格式传输，具有扩展读取权限的攻击者可以查看这些密码。

仅会影响2.236（包括 2.235.x LTS）之前的 Jenkins，因为 Jenkins 2.236 引入了安全性强化功能，可以透明地加密和解密用于 Jenkins 密码表单字段的数据。

截至本公告发布之时，尚无修复程序。

风险等级

CVE-2020-2249 低风险
CVE-2020-2239 低风险
CVE-2020-2241 中风险
CVE-2020-2242 中风险
CVE-2020-2250 中风险
CVE-2020-2251 中风险
CVE-2020-2240 高风险
CVE-2020-2247 高风险
CVE-2020-2248 高风险
CVE-2020-2246 高风险
CVE-2020-2245 高风险
CVE-2020-2243 高风险
CVE-2020-2238 高风险
CVE-2020-2244 高风险

影响版本

Build Failure Analyzer Plugin <= 1.27.0
Cadence vManager Plugin <= 3.0.4
database Plugin <= 1.6

Git Parameter Plugin <= 0.9.12
JSGames Plugin <= 0.2
Klocwork Analysis Plugin <= 2020.2.1
Parameterized Remote Trigger Plugin <= 3.1.3
SoapUI Pro Functional Testing Plugin <= 1.3
SoapUI Pro Functional Testing Plugin <= 1.5
Team Foundation Server Plugin <= 5.157.1
Valgrind Plugin <= 0.28

修复版本

Build Failure Analyzer Plugin should be updated to version 1.27.1
Cadence vManager Plugin should be updated to version 3.0.5
database Plugin should be updated to version 1.7
Git Parameter Plugin should be updated to version 0.9.13
Parameterized Remote Trigger Plugin should be updated to version 3.1.4
SoapUI Pro Functional Testing Plugin should be updated to version 1.4

等待修补版本

JSGames Plugin
Klocwork Analysis Plugin
SoapUI Pro Functional Testing Plugin
Team Foundation Server Plugin
Valgrind Plugin

修复建议

官方发布部分升级插件修复该漏洞，但是由于部分插件缺少修复版本，腾讯云安全建议您：
更新对应 Jenkins 插件（由于明文存储漏洞为本地漏洞，需等待插件更新）。
由于 Jenkins 的敏感性，建议 Jenkins 不对外开放，如果有公网访问需求，可以在腾讯云 Web 应用防火墙上面 配置 IP 白名单 等访问策略。
推荐企业用户采取腾讯云 Web 应用防火墙检测并拦截 Jenkins 9月安全更新通告中基于网络的漏洞攻击。
腾讯云 Web 应用防火墙（Web Application Firewall）已支持拦截防御 Jenkins 9月安全更新通告内包含的漏洞。

参考信息

官方通告如下:

Jenkins Security Advisory 2020-09-01

CVE-2020-2238

CVE-2020-2239

CVE-2020-2240

CVE-2020-2241

CVE-2020-2242

CVE-2020-2243

CVE-2020-2244

CVE-2020-2245

CVE-2020-2246

CVE-2020-2247

CVE-2020-2248

CVE-2020-2249

CVE-2020-2250

CVE-2020-2251

CloudBees Jenkins XSS 漏洞（CVE-2020-2246）

CloudBees Jenkins XSS 漏洞（CVE-2020-2243）

CloudBees Jenkins XXE 漏洞

Apache Struts2 远程代码执行漏洞公告（CVE-2019-0230、CVE-2019-0233）

最近更新时间：2022-06-23 11:14:27

2020年8月13日，腾讯安全团队监测到 Apache Struts 官方发布安全公告，披露 S2-059 Struts 远程代码执行漏洞，以及 S2-060 Struts 拒绝服务漏洞。

漏洞详情

Apache Struts2 框架是一个用于开发 Java EE 网络应用程序的 Web 框架。
S2-059 Struts 远程代码执行漏洞（CVE-2019-0230），在不规范的使用某些 tag 等情况下，可能存在 OGNL 表达式注入，从而引发远程代码执行漏洞。
S2-060 Struts 拒绝服务漏洞（CVE-2019-0233），使得在上传文件并对其进行操作的时候，造成拒绝服务漏洞攻击。

影响版本

Apache Struts 2.0.0 - 2.5.20

安全版本

Apache Struts >= 2.5.22

修复建议

根据漏洞相关信息，腾讯安全建议您：
将 Apache Struts 框架升级至最新版本。
使用腾讯云 Web 应用防火墙，腾讯云 Web 应用防火墙是基于 AI 的一站式 Web 安全解决方案。 S2-059 漏洞最典型的特征就是该漏洞会用到 OGNL 语言，在此之前腾讯安全技术团队针对 ONGL 表达式进行了定向攻坚，针对 OGNL 表达式的攻击进行了定向封堵，并集成到 Web 应用防火墙中，因此只要是根据 OGNL 表达式来攻击的漏洞，Web 应用防火墙都可以直接防御。
同时腾讯云 Web 应用防火墙的智能引擎也针对 sql、xss 和命令执行等类型攻击进行智能防御，配合 AI 技术对未知的安全漏洞威胁进行合理有效的封堵，为业务保驾护航。

参考信息

官方公告信息：

CVE-2019-0230

CVE-2019-0233

Apache SkyWalking SQL 注入漏洞安全风险公告（CVE-2020-13921）

最近更新时间：2022-06-23 11:14:27

2020年8月5日，腾讯蓝军（force.tencent.com）研究发现 Apache SkyWalking 存在 SQL 注入漏洞（漏洞编号：CVE-2020-13921），目前官方已发布新版本修复该漏洞。
为避免您的业务受影响，腾讯云安全建议您及时开展安全自查，如在受影响范围，请您及时进行更新修复，避免被外部攻击者入侵，详情请参见 影响版本。

漏洞详情

Apache SkyWalking 是一款应用性能监控（APM）工具，对微服务、云原生和容器化应用提供自动化、高性能的监控方案。其官方网站显示，大量的国内互联网、银行及民航等领域的公司在使用此工具。
在 SkyWalking 多个版本中，默认开放的未授权 GraphQL 接口，通过该接口，攻击者可以构造恶意的请求包进行SQL注入，从而导致用户数据库敏感信息泄露。鉴于该漏洞影响较大，建议企业尽快修复。

风险等级

高风险

漏洞风险

通过 SQL 注入，攻击者可以在服务器上窃取敏感信息。

影响版本

Apache SkyWalking 6.0.0 - 6.6.0
Apache SkyWalking 7.0.0
Apache SkyWalking 8.0.0 - 8.0.1

修复补丁

Apache SkyWalking 8.1.0

修复建议

官方已发布新版本修复该漏洞，腾讯云安全建议您：
推荐方案：升级到 Apache SkyWalking 8.1.0 或更新版本。
临时缓解方案：如暂时无法升级，作为缓解措施，建议不要将 Apache SkyWalking 的 GraphQL 接口暴露在外网，或在 GraphQL 接口之上增加一层认证。
推荐企业用户：采取腾讯安全产品检测并拦截 Apache SkyWalking SQL 注入漏洞的攻击。
腾讯云 Web 应用防火墙已支持拦截防御 SkyWalking SQL 注入漏洞攻击。

参考信息

如有需要，您可以在 相关 GitHub 链接 中，下载相关参考漏洞。