Web 应用防火墙

动态与公告

产品文档

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

动态与公告

产品动态

最近更新时间：2021-08-03 10:09:07

2021-07

动态名称	动态描述	发布时间	相关文档
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。	2021-7-30	BOT 行为管理
情报中心	让客户快速了解最新的威胁情报。	2021-07-16	情报中心

2021-04

动态名称	动态描述	发布时间	相关文档
前端对抗发布	BOT 能力增强，新增前端对抗，通过客户端动态安全验证技术，对业务请求的每个客户端生成唯一 ID，检测客户端对 Web 或 H5 页面访问中可能存在机器人和恶意爬虫行为，保护网站业务安全。	2021-04-24	前端对抗
IPv6 支持	SAASWAF 和 CLBWAF 均支持 IPv6 接入，提供和 IPv4 同等的防护能力。	2021-04-24	-

2021-03

动态名称	动态描述	发布时间	相关文档
多实例支持	满足有多个账号，多套 WAF 的统一管控需求，特别适合重保场景，减轻安全运营团队来回切换的成本，提升运营效率。	2021-03-24	实例列表
CC 功能增强	在 IP + URL 和 session + URL 组合频率的基础上，支持更多的条件，满足客户精细化频率控制要求，提升 CC 防御频率效率。	2021-03-24	-

2021-02

动态名称	动态描述	发布时间	相关文档
防泄漏功能增强	新增支持自定义关键字（支持正则）过滤、动作处理支持敏感信息部分替换或者全部替换。新增对网站返回的状态码，进行阻断或者告警处理，满足合规要求。	2021-02-24	防信息泄露

2021-01

动态名称	动态描述	发布时间	相关文档
信誉防护策略	新增信誉防护策略，启用后 WAF 将对代理、扫描器、恶意情报 IP 等恶意访问请求进行防护。	2021-01-18	IP 封禁管理
攻击 IP 惩罚	自动阻断在短时间内发起多次 Web 攻击（规则引擎触发）的客户端 IP，阻止所有请求一段时间，阻断日志可以在攻击日志中查看。	2021-01-18	IP 封禁管理

2020-12

动态名称	动态描述	发布时间	相关文档
业务安全解决方案	联合天御推出 WAF 业务安全方案，通过账号信息提取及风险评估，对注册保护、登录保护及活动防刷等场景进行精准防护。	2020-12-17	业务安全
API 安全	支持全新 API 安全解决方案，您添加 API 接口或上传 API 描述文件到 WAF，将对 API 进行安全保护。	2020-12-17	API 安全

2020-11

动态名称	动态描述	发布时间	相关文档
弹性计费	支持为 WAF 实例开通弹性后计费，对超出 WAF 套餐规格的 QPS 进行正常防护。	2020-11-17	弹性计费
全新规则管理	支持全新规则，支持规则开通，基于 URL 的规则白名单进行设置。	2020-11-10	规则引擎

2020-10

动态名称	动态描述	发布时间	相关文档
独享版本发布	推出资源独享版本，满足大客户特殊定制化 Web 和 API 服务安全防护。	2020-10-27	计费概述
全新攻击日志检索	基于日志服务提供全新攻击日志检索能力。	2020-10-27	-

2020-09

动态名称	动态描述	发布时间	相关文档
WAF 接入支持自动检查	自动检查域名接入状态，对源站、集群及证书等进行高可用保障，自动处理域名故障，优化客户体验。	2020-09-12	-

2020-07

动态名称	动态描述	发布时间	相关文档
CLB WAF 支持海外地区	CLB WAF 各地域清洗模式上线，支持亚洲及欧洲等地区，支持 IPv6 防护。	2020-07-28	支持地域
日志支持百万级下线	攻击日志能力升级，支持百万级日志下载。	2020-07-28	-

2020-06

动态名称	动态描述	发布时间	相关文档
规则引擎优化	引入全新旁路规则检测引擎，Web 入侵检测能力全面提升，全区域开放。	2020-06-17	-
SCDN 产品方案发布	联合 CDN 发布 SCDN 产品方案，部分 CDN 节点具备 WAF 安全能力。	2020-06-04	安全加速

2020-05

动态名称	动态描述	发布时间	相关文档

云监控功能上线	WAF 接入云监控，可通过云监控配置支持 QPS、Web 攻击、CC 攻击和 WAF 状态码告警（4xx、5xx）。	2020-05-17	-
API3.0 发布	发布 API3.0，WAF 所有功能均可通过 API 进行操作和使用，如有需要，请 联系我们 进行支持。	2020-05-11	-

2020-04

动态名称	动态描述	发布时间	相关文档
AI 引擎优化	AI 引擎性能和算法全面提升，支持全新旁路检测架构。	2020-04-27	AI 引擎

2020-03

动态名称	动态描述	发布时间	相关文档
攻击概览优化	攻击概览支持 TOP Web 攻击和 CC 攻击域名排序。	2020-03-15	-
访问日志优化	支持访问日志使用量统计和访问总数统计。	2020-03-15	访问日志

2020-01

动态名称	动态描述	发布时间	相关文档
发布 CLBWAF 全新产品方案	• 通过和腾讯云负载均衡集群进行联动，实现转发和安全防护分离，WAF 对经过负载均衡的 HTTP 和 HTTPS 进行旁路检测和威胁状态同步，实现网站安全防护。 • 支持南京清洗模式，支持广州、北京、上海镜像模式，灰度开放。	2020-01-15	负载均衡型 WAF

2019-12

动态名称	动态描述	发布时间	相关文档
Webshell 检测开	新增独立 Webshell 检测引擎。	2019-	-

放		12-22	
BOT2.0 发布	• 优化 BOT 概览和详情，展示更加合理、内容丰富，搜索更易于使用，BOT 记录信息更完整，可读性更强。 • 增强 BOT 检测能力和防护策略，新增协议特征、IP 情报特征和自定义会话特征等多种检测维度，更有利于恶意 BOT 识别和对抗。 • 优化 BOT 策略动作处理，动作实时生效，不再依赖 WAF 自定义策略，支持设置策略动作生效时间，新增人机识别、重定向动作处理。	2019-12-09	BOT 概览

2019-09

动态名称	动态描述	发布时间	相关文档
支持新购 QPS 包和日志服务包	用户可以根据需要购买安全日志服务包和 QPS 扩展包，满足业务扩容需求。	2019-09-18	购买指南
支持非标端口	新增企业版和旗舰版非标端口，旗舰版支持非标端口定制。	2019-09-18	端口支持相关

2019-08

动态名称	动态描述	发布时间	相关文档
日志服务	WAF 支持记录和存储网站访问日志6个月，最近30天访问日志查询和下载，满足等保合规要求。	2019-08-09	访问日志
智能CC防护	结合网站历史数据，用户异常访问行为和源站负载情况生成自动防御策略，防护 CC 攻击。	2019-08-09	CC 防护设置2.0
地域封禁增强	WAF 支持对境外219个国家和地区选择进行地域封禁。	2019-08-09	地域封禁
新增自定义拦截页面定制	用户可以自定义 WAF 拦截返回页面，如有需要，请 联系我们 进行支持。	2019-08-09	-

Web2.0 发布公告

最近更新时间：2021-12-03 17:49:01

自2021年10月15日起，Web 应用防火墙逐步灰度上线 Web2.0控制台和防护能力版本升级内容。在经过充分验证后，于2021年11月30日起面向用户正式发布。

新版发布后，新用户将立刻体验到全新的实例管理、域名接入、防护配置中心、日志服务，以及安全报表管理等多模块的 Web2.0控制台。为了兼顾老用户的配置体验，我们向老用户同时提供了新、旧两个 Web 控制台版本的域名接入和防护配置页面（新用户只看到新版本）；新老版本页面均具备良好的兼容性，不会影响用户已接入和配置的业务。

为进一步聚焦提升产品能力，优化用户接入和防护配置体验，于2021年12月20日起，我们将陆续取消老版域名接入和配置页面，全部升级为新的域名接入、防护配置页面，升级替换过程中不会影响业务和产品配置的连续性。

本次 Web2.0升级后，您将获得以下产品能力和配置体验：

域名接入全面升级、更快捷

域名管理升级

支持多实例统一管理，助力用户提升日常安全运维效率。

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

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

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。

IPV6 业务接入

一键开关 IPv6 服务和防护，为网站防御 IPv6 环境下发起的攻击，并可帮助 IPV4 源站快速实现 IPV6 服务化改造，助力业务合规合法。

防护能力升级

一键开关防护

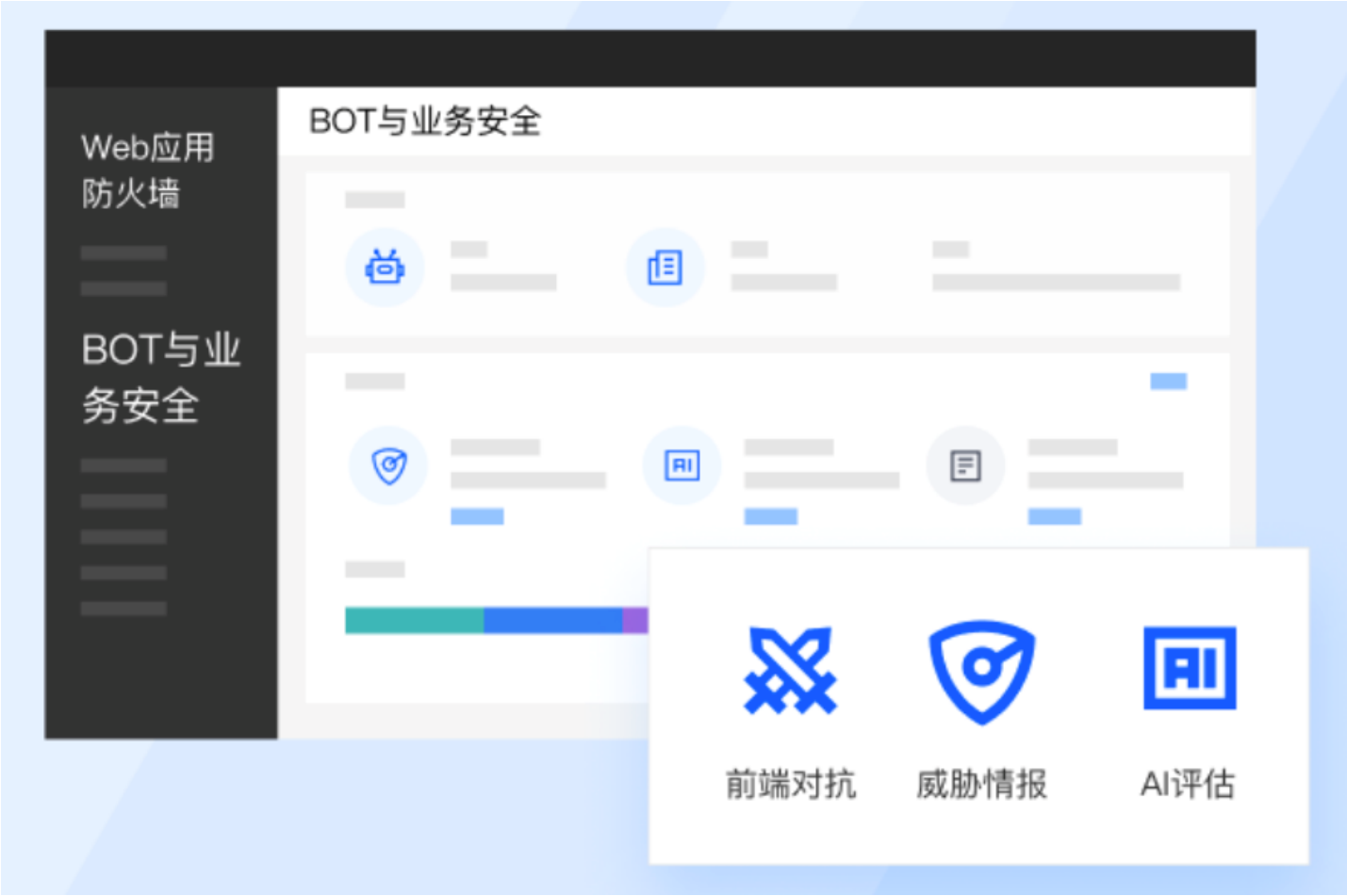
支持一键开启和关闭全部防护模块，以及部分防护功能模块的防护能力，助力用户快速处置日常运维过程中的业务问题排查，虽缩短定位周期，保障业务连续性。

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。

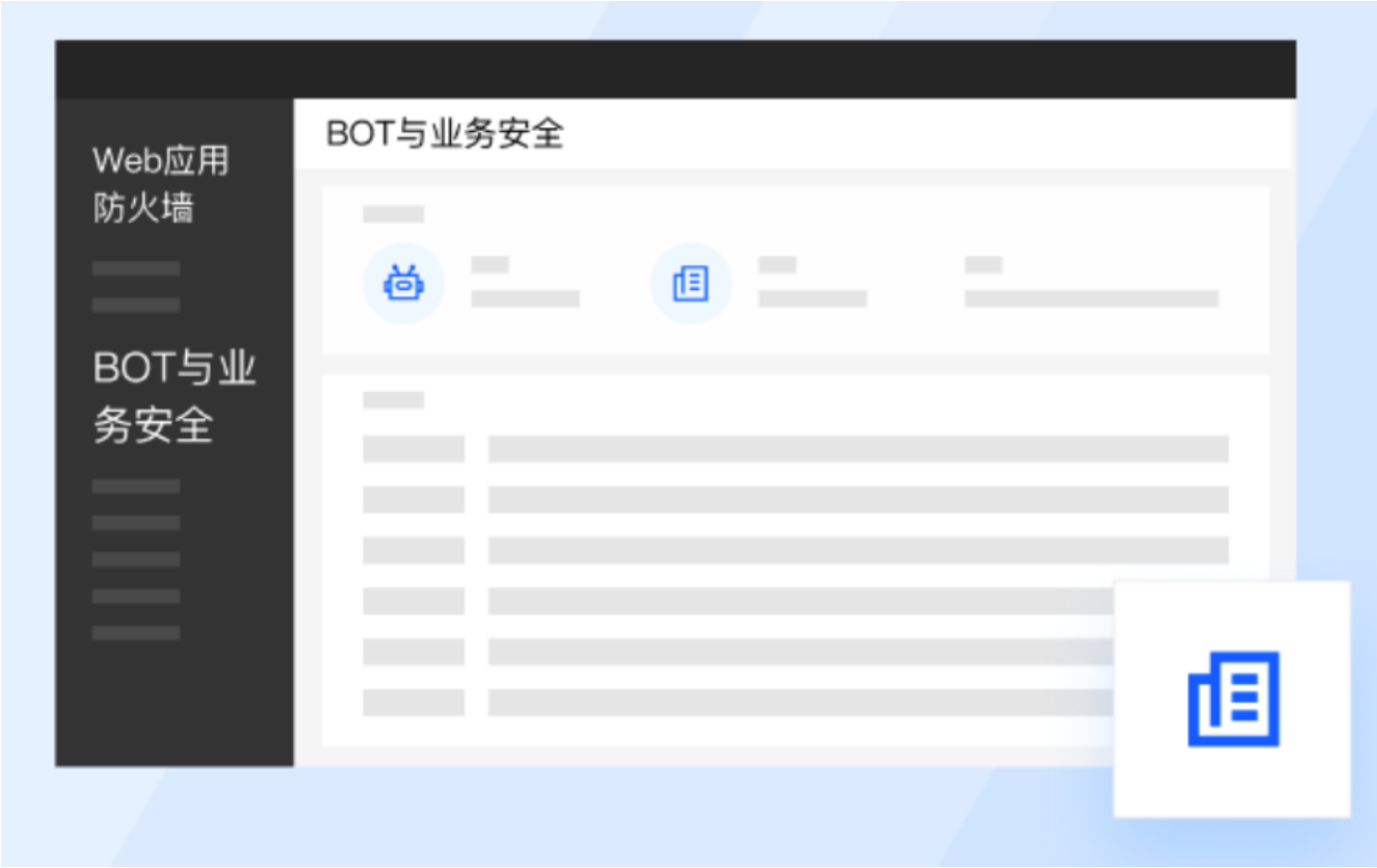
BOT2.0商业化发布

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。



业务安全商业化发布

联合腾讯天御风控引擎，基于人工智能技术和腾讯20年风控实战沉淀的手机号、微信 openid、QQ openid、设备号、IP 等多个维度情报数据，帮助您快速识别和处置机器注册、机器刷单登录、羊毛党抢购等恶意欺诈活动。


Web应用
防火墙
BOT与业
务安全
BOT与业务安全

安全公告
Weblogic Console HTTP 协议远程代码执行漏洞公告

最近更新时间：2020-11-03 16:29:35

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：2020-10-12 16:28:46

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：2020-10-12 16:28:51

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：2020-10-12 16:28:56

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：2020-10-12 16:29:05

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：2020-10-12 16:29:22

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：2020-10-12 16:29:31

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：2021-01-08 16:18:42

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。

Fastjson 远程拒绝服务漏洞防护公告

最近更新时间：2020-12-24 15:44:05

漏洞名称

Fastjson 远程拒绝服务漏洞

影响版本

Fastjson 1.2.60 以下版本

漏洞详情

近日，腾讯云安全中心 监测到开源 JSON 解析库 Fastjson 1.2.60 以下版本存在字符串解析异常，攻击者可利用该漏洞，将精心构造的恶意请求包，发送至使用到 Fastjson 的服务器，耗尽服务器内存及 CPU 等资源，导致服务不可用。目前该漏洞相关利用代码已被公开，建议尽快升级处理。

官方修复建议

拒绝服务安全漏洞涉及之前所有 Fastjson 版本，建议将 Fastjson 升级到最新1.2.60版本。

防护建议

腾讯云 Web 应用防火墙攻击防护规则中，已经包含该漏洞的防护规则，操作步骤如下：

1. 登录 腾讯云 Web 应用防火墙控制台 ，在左侧导航栏中，选择【 Web 应用防火墙 】>【 防护设置 】，在域名列表中，选择需要防护的域名，在操作栏单击【 防护配置 】。

2. 在基础设置页面，将 WAF 防护状态的“规则引擎”设置为【拦截】即可防御。

更多信息请参见【安全预警】Fastjson < 1.2.60 远程拒绝服务漏洞风险预警 。