Web 应用防火墙

安全公告

产品文档

腾讯云

文档目录

安全公告
Exchange Server 命令执行漏洞的安全防护公告

最近更新时间：2020-10-13 11:48:20

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：2020-10-13 11:48:20

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：2020-10-13 11:48:20

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：2020-10-13 11:48:20

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：2021-01-06 11:03:48

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

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

最近更新时间：2020-10-13 11:48:21

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：2020-10-13 11:48:21

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。