**Spring Cloud Zuul组件\_1.4.7版本\_安全漏洞处置方案**

**基础技术中心**

**2025年8月**

# 修订记录

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **编号** | **日期** | **描述** | **版本** | **作者** | **审核** | **发布日期** |
| 1 | 2025-08-19 | 建立文档 | 1.0 | 汤王 |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |

如无中国建设银行的书面许可，任何人都无权复制或利用。

**目 录**

[修订记录 2](#_Toc3833)

[1. 漏洞来源 4](#_Toc15241)

[2. 影响分析 4](#_Toc14050)

[3. 漏洞等级 4](#_Toc23722)

[4. 漏洞检测方法 4](#_Toc4877)

[5. 处置策略 5](#_Toc27430)

[5.1. 临时缓制措施 5](#_Toc22980)

[5.2. 正式修复方案 6](#_Toc12063)

[6. 升级路径与建议 6](#_Toc31133)

[7. 联系支撑人员 7](#_Toc28646)

# 漏洞来源

本处置方案主要针对官方披露的 Spring Cloud Zuul 路径穿越（Directory Traversal）漏洞，漏洞编号为CVE-2019-3799。该漏洞允许攻击者通过构造恶意的 URL 请求，访问到 Zuul 网关服务器上文件系统的任意文件。

# 影响分析

* **漏洞原理**：当 Zuul 路由配置使用了通配符（如 /\*\*）时，其反向代理的特性未能正确处理和净化 URL 中的路径遍历序列（如 ../）。攻击者可以发送一个精心构造的 HTTP 请求，利用 ..%2f (URL编码的 ../) 等字符绕过路由规则，从而读取到部署 Zuul 服务器上的敏感文件，例如配置文件、源代码、系统文件（如 /etc/passwd）等 。
* **影响范围**：
  + Spring Cloud Edgware 版本 SR5 及更早版本（对应 Zuul 1.4.6.RELEASE 及更早版本）。
  + Spring Cloud Finchley 版本 SR3 及更早版本。
  + Spring Cloud Dalston 版本 SR10 及更早版本。

**严重程度**：该漏洞可导致敏感信息泄露，对系统的机密性造成严重威胁 。

# 漏洞等级

根据通用漏洞评分系统（CVSS 3.0），该漏洞的评分为7.5，属于 高（High） 风险等级 。

# 漏洞检测方法

可通过以下两种方式确认当前运行的 Zuul 实例是否存在此漏洞 。

* 方法一：版本检查（推荐）  
  检查项目 pom.xml (Maven) 或 build.gradle (Gradle) 文件中 spring-cloud-starter-zuul 或 spring-cloud-starter-netflix-zuul 依赖的版本。如果版本号为 1.4.6.RELEASE 或更低，则系统存在漏洞。
* 方法二：主动探测验证  
  假设您的 Zuul 网关地址为 http://zuul.example.com，且存在一个路由 my-app 指向某个后端服务。可以执行以下命令：  
  # 尝试读取 /etc/passwd 文件

curl -v --path-as-is http://zuul.example.com/my-app/..%2f..%2f..%2f..%2fetc/passwd

****参数说明**​**

| **参数** | **作用** |
| --- | --- |
| -v | 显示详细请求/响应过程（调试模式） |
| --path-as-is | ​****关键参数****​：禁止curl自动标准化路径，保持..%2f原样发送 |
| ..%2f | URL编码的../，用于尝试穿越目录 |

* + **存在漏洞的响应**：如果响应内容中包含类似 root:x:0:0:root:/root:/bin/bash 的系统用户信息，则确认系统存在漏洞。
  + **已修复的响应**：已修复的系统（如 1.4.7 版本）会正确处理该请求，通常会返回 404 Not Found 或 400 Bad Request 错误。

# 处置策略

## 临时缓制措施

在无法立即升级版本的情况下，可采取以下一种或多种措施进行临时防护 ：

1. **WAF/Nginx 规则拦截**：在 Zuul 网关上层的 Web 应用防火墙（WAF）或 Nginx 等接入层设备上配置规则，拒绝包含路径遍历特征（如 ../、..%2f、..%c0%af 等）的 URL 请求。
   * **Nginx 示例规则**：  
     Nginx  
     if ($request\_uri ~\* "/\.\./") {  
      return 403;  
     }
2. **收紧路由规则**：审查所有 Zuul 的路由配置，避免使用过于宽泛的 /\*\* 通配符。尽可能使用更具体的路径前缀，减小攻击面。

## 正式修复方案

官方已发布修复版本，彻底的解决方案是升级 Spring Cloud Zuul 的依赖版本 。

1. 升级组件版本：  
   在项目的 pom.xml 文件中，将 spring-cloud-dependencies 的版本升级到包含修复后 Zuul 的版本。例如，如果您正在使用 Edgware 版本，应至少升级到 Edgware.SR6。  
   XML  
   <properties>  
    <spring-cloud.version>Edgware.SR6</spring-cloud.version>  
   </properties>  
     
   <dependencyManagement>  
    <dependencies>  
    <dependency>  
    <groupId>org.springframework.cloud</groupId>  
    <artifactId>spring-cloud-dependencies</artifactId>  
    <version>${spring-cloud.version}</version>  
    <type>pom</type>  
    <scope>import</scope>  
    </dependency>  
    </dependencies>  
   </dependencyManagement>  
     
   升级后，spring-cloud-starter-netflix-zuul 将自动引入修复后的 1.4.7.RELEASE 版本。
2. **重新编译并部署**：升级依赖后，需重新编译应用代码，并将其部署到所有生产环境节点。

# 升级路径与建议

* **直接升级路径**：建议所有使用受影响版本的团队，直接将 spring-cloud-dependencies 升级到包含 Zuul 1.4.7.RELEASE 的发行版（如 Edgware.SR6） 。该版本为补丁修复，API 兼容性高，升级风险较低。
* **长期建议**：Spring Cloud Zuul 1.x 已进入维护模式，不再积极开发新功能。官方推荐新项目使用 **Spring Cloud Gateway** 作为下一代网关解决方案。建议在项目迭代计划中，规划从 Zuul 1.x 迁移到 Spring Cloud Gateway 的任务。

# 联系支撑人员

如果在漏洞处置或版本升级过程中遇到任何问题，请联系基础技术中心：

* **联系人**：汤王
* **电话**：15852051279
* **邮箱**：tangwang.jkjs@ccbft.com