

CVE-2022-22947 正式环境修复说明

BladeX 2.7.2, Spring Cloud Hoxton.SR9。漏洞入口是 Gateway 的 `/actuator/gateway`。正式环境关闭该端点并重启 Gateway 即可，不用发版，不用升级 Spring Cloud Gateway。

动态路由走 Nacos，不依赖这个端点。`web/vue.config.js` 只影响本地前端代理，正式环境不要改。

一、要改的配置

Nacos Group: `DEFAULT_GROUP`。命名空间用对应环境自己的 namespace。

Data ID	怎么改
<code>blade.yaml</code>	只替换已有的 <code>management</code> 段
<code>blade-gateway.yaml</code>	没有就新建；已有则写入下面第 2 节
<code>blade-gateway-prod.yaml</code>	仅当这个文件已经存在时，写入同样内容。环境配置优先级更高

不要改 `custom.properties`。那是 Nacos 进程自己的配置，关不掉 Gateway。

1. `blade.yaml`

只改 `management` 这一段。不要整文件覆盖。全文只能有一个根级 `management:`。`knife4j` 保持原样，并且仍在根上，`enable` 仍为 `true`。

```
#对外暴露端口
management:
  endpoints:
    web:
      exposure:
        include: health,info
  endpoint:
    health:
      show-details: always
  gateway:
    enabled: false
```

监控要抓 Prometheus 时，`include` 写成 `health,info,prometheus`。不要写回 `*`。

发布前确认没有第二段 `management:`。Nacos 若提示 `duplicate key management`，删掉后贴的那一段，只保留上面这一段。

2. blade-gateway-prod.yaml

```
management:
  endpoint:
    gateway:
      enabled: false
  endpoints:
    web:
      exposure:
        include: health,info
```

若已存在 `blade-gateway-prod.yaml`，把这段同样写入该文件。

二、重启

配置发布后，重启全部 Gateway 实例。端点在进程启动时注册，只刷新配置不会关掉。Kubernetes 上滚动重启 Gateway 的全部副本。

其他业务服务不用为这个漏洞单独发版。若重启后报 `knife4j.enable` 或 `OpenApiExtensionResolver`，说明 `blade.yaml` 里的 `knife4j.enable: true` 丢了，或被缩进到 `management` 下面。按第一节恢复后再启动。

三、测试案例

`<host>`、`<port>` 换成正式环境访问 Gateway 的地址。扫描入口是 `10.244.198.64:30003`，以实际 NodePort 或 Ingress 为准。`<token>` 用登录成功后请求头 `Blade-Auth` 的完整值，包含前面的 `bearer`。

案例 1：健康检查仍然可用

```
curl -i http://<host>:<port>/actuator/health
```

通过：HTTP **200**，正文含 `"status":"UP"`。

案例 2：漏洞端点已关闭

```
curl -i http://<host>:<port>/actuator/gateway -H "Blade-Auth: <token>"
```

通过：HTTP **404**。

失败：HTTP **200**，并且返回路由列表。说明端点仍开启，配置未生效或 Gateway 未重启。

案例 3：端点子路径已关闭

```
curl -i http://<host>:<port>/actuator/gateway/routes -H "Blade-Auth: <token>"
```

通过：HTTP **404**。

判定

三条都通过才算修复完成。不带令牌访问得到 **401** 不能算通过，那只说明未登录被拦住，端点可能还在。

本地 127.0.0.1:6003 已测过，案例 1 为 200，案例 2、案例 3 为 404。

案例 4：登录未受影响

```
curl -i http://<host>:<port>/blade-auth/oauth/captcha
```

通过：HTTP 200，正文含 key 和 image。再用租户 000000 的管理员账号从页面登录一次。

四、修复前已被入侵时

关掉端点只能阻止再次写入。若该 Gateway 在修复前已被写入内存马，用当前构建重新拉起全部 Gateway 进程，并检查 Nacos 里的路由配置有没有异常新增路由。