/

20211207

-
-
-
-
-

-
-
-
-
-
-

-
  -
  -
  -
-
  -
  - BUG
  -
  -
  -
  -
  - IP
-
  -
  -
-
  -
  -
  -
  -
-
  -
-
  -
  -
  -
  -
-
  -
  -
  -
  - IDID+IP
-
  - JAR
  - JAR
  - ticketcodeIP
  -
  -
  -
  -
  -
  -
-

    -
    - c/c++
    -
-
    -

- /
    -
    - 100%
    - 40%
    - 10%
    -
- /
- /
- /
- sevnsevn@fanruan.com
- sevnhugh
- /

- **202211**

	1) OpenSSLRAND_bytes 2) OpenSSL FIPSDRBG 3) JDKjava.security.SecureRandom 4Unix/dev/random 5WindowsCryptGenRandom
	MD5/DES/3DESTLS/SSH3DESK1K2K3/HMAC-SHA2-256-96/HMAC-SHA1-96/HMAC-MD5/HMAC-MD5-96/SSHCBC//DH512/DH1024 /SKIPJACK/RC2/RSA1024/MD2/MD4 1MD5“/hash-only/HMAC//” 2SHA1“/hash-only”“HMAC//”
	1AES128 2AES128OFBCTR 3RSA20483072) 4SHA2256 5DH20483072) 6HMACHMAC-SHA2 PBKDF2HMAC 1PBKDF2100001000 2Saltsalt16 3HASH(||)HMAC()HASH(XOR salt)