



Fork Bomb For Flutter

Nikiforov Philip

Senior Mobile Application Security Researcher, Positive Technologies

@impact_l

Moscow, August 25, 2022



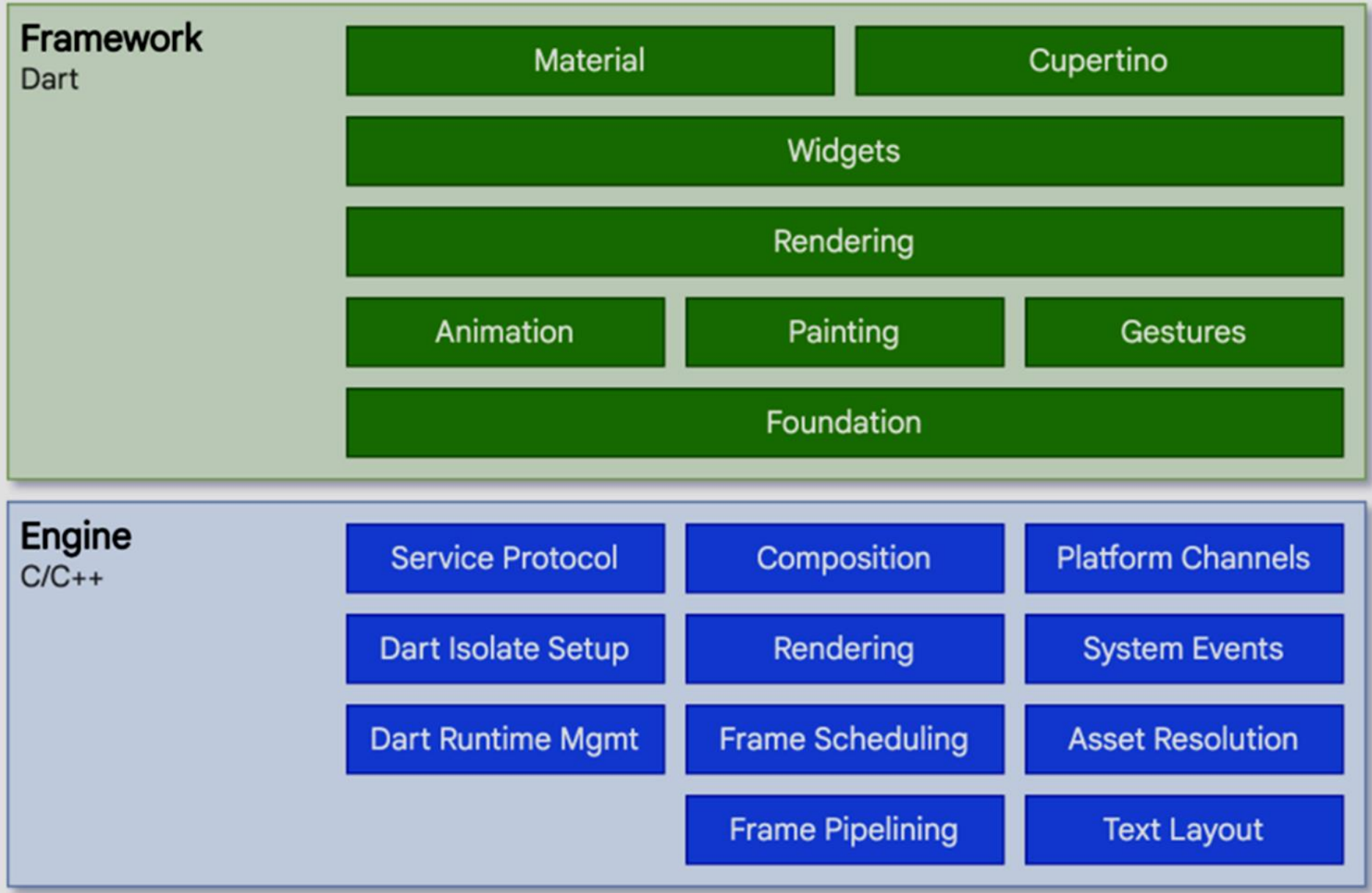
About Me



- AppSec Engineer at Positive Technologies
- Security Researcher
- Telegram @impact_l
- Member of PT SWARM
- BugBounty hackerone.com/shell_c0de

Agenda

1. Overview of Flutter
2. How to build simple mobile app
3. About a specific approach for Flutter reverse engineering
4. Demonstration on the BMW app: intercepting traffic in BurpSuite and capturing function arguments via Frida



```
~/flutter_app/android$ ./gradlew -Pverbose=true -Ptarget-platform=android-arm64 -Ptarget=lib/main.dart assembleRelease
```



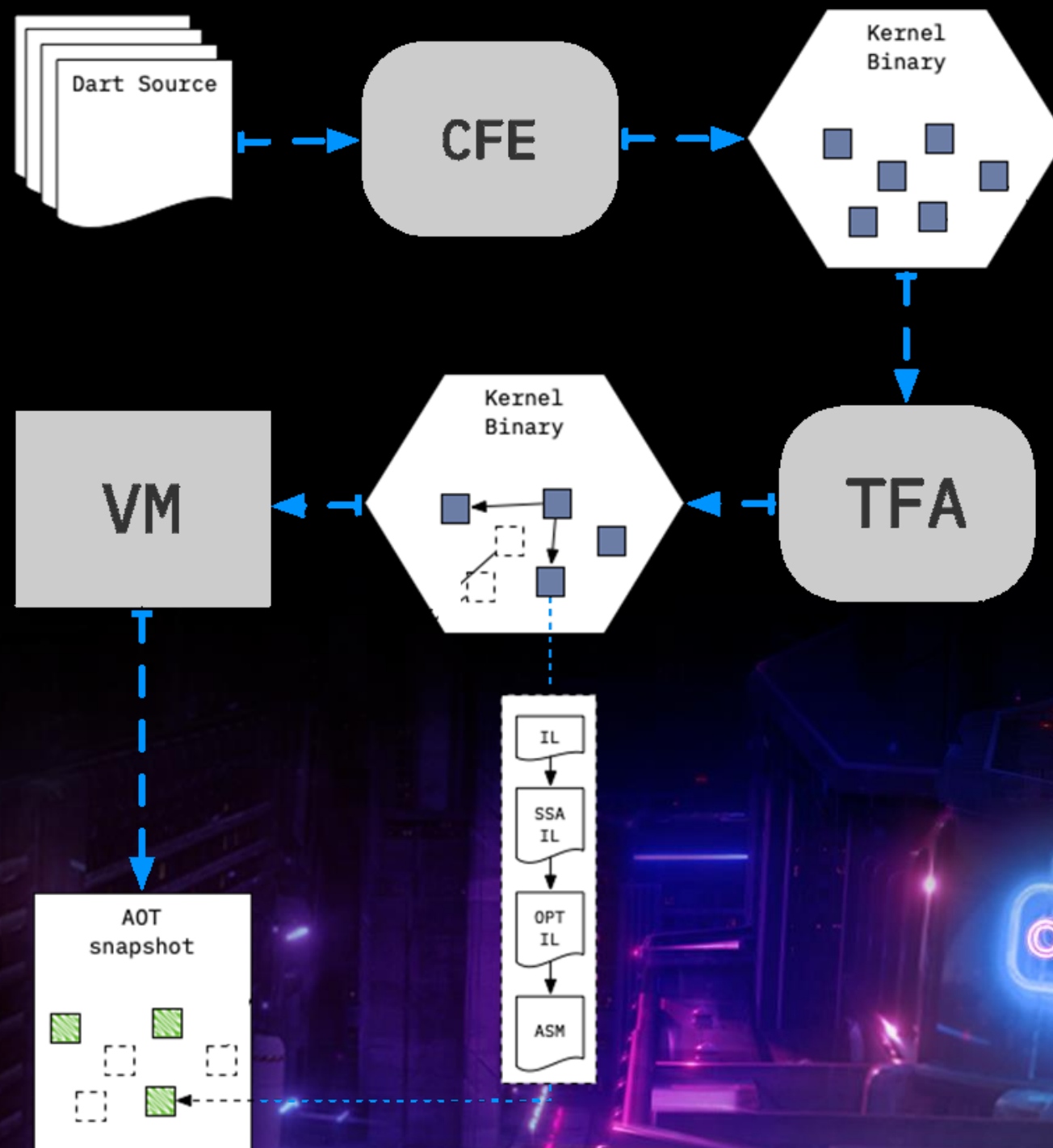
- [+11 ms] dart-sdk/bin/dart artifacts/engine/linux-x64/frontend_server.dart.snapshot --sdk-root artifacts/engine/common/flutter_patched_sdk_product/ --target=flutter -Ddart.developer.causal_async_stacks=false -Ddart.vm.profile=false -Ddart.vm.product=true --bytecode-options=source-positions --aot --tfa --packages .packages --output-dill app.dill package:flutter_app/main.dart
- [+7108 ms] kernel_snapshot: Complete
- [+3 ms] executing: artifacts/engine/android-arm64-release/linux-x64/gen_snapshot --deterministic --snapshot_kind=app-aot-elf --elf=libapp.so --strip --no-causal-async-stacks --lazy-async-stacks app.dill
- [+3668 ms] android_aot_release_android-arm64: Complete

Dart Kernel Binary

```
dart-sdk/bin/dart artifacts/engine/linux-  
x64/frontend_server.dart.snapshot  
  
--sdk-root  
artifacts/engine/common/flutter_patched_sdk_product  
  
--target=flutter --tfa  
  
-Ddart.developer.causal_async_stacks=false  
  
-Ddart.vm.profile=false  
  
-Ddart.vm.product=true  
  
--bytecode-options=source-positions  
  
--aot  
  
--packages .packages --output-dill app.dill  
package:flutter_app/main.dart
```

AOT Snapshot

```
artifacts/engine/android-arm64-  
release/linux-x64/gen_snapshot  
  
--deterministic  
--snapshot_kind=app-aot-elf  
--elf=libapp.so  
--strip --no-causal-async-stacks --  
lazy-async-stack  
app.dill
```

Release.apk



- |— AndroidManifest.xml
- |— assets
 - | — flutter_assets
 - | — AssetManifest.json
- |— classes.dex — // Java (Dalvik Executable)
- |— kotlin — // kotlin Metadata
- |— lib
 - | — arm64-v8a
 - | — libapp.so — // Dart code (App AOT Snapshot)
 - | — libflutter.so — // Flutter Engine (stripped version of Dart VM)
- |— META-INF
- |— res
- |— resources.arsc

Segments

```
~$ readelf -Ws libapp.so
```

Symbol table '.dynsym' contains 6 entries:

Num:	Value	Size	Type	Bind	Ndx	Name
0:	0000	0	NOTYPE	LOCAL	UND	
1:	1000	8	FUNC	GLOBAL	1	__kDartBSSData
2:	2000	17792	FUNC	GLOBAL	2	__kDartVmSnapshotInstructions
3:	7000	0x1f89c0	FUNC	GLOBAL	3	__kDartIsolateSnapshotInstructions
4:	200000	32288	FUNC	GLOBAL	4	__kDartVmSnapshotData
5:	208000	0x18c180	FUNC	GLOBAL	5	__kDartIsolateSnapshotData

Versions

Stable , Beta , Dev

storage.googleapis.com:

```
{  
  "hash": "8f89f6505b941329a864fef1527243a72800bf4d",  
  "channel": "beta",  
  "version": "1.25.0-8.1.pre",  
  "release_date": "2020-12-16T21:55:19.340490Z",  
  "archive": "beta/linux/flutter_linux_1.25.0.pre.tar.xz",  
},
```


Google Storage

../flutter/8f89f6505b941329a864fef1527243a72800bf4d/linux-x64/artifacts.zip
../flutter/8f89f6505b941329a864fef1527243a72800bf4d/flutter_patched_sdk_product.zip
../flutter/8f89f6505b941329a864fef1527243a72800bf4d/android-arm64-release/linux-x64.zip
../flutter/8f89f6505b941329a864fef1527243a72800bf4d/dart-sdk-linux-x64.zip

OverviewSteps & LogsRelated BuildsTimelineBlamelist

Build succeeded

Steps & Logs (View in Steps Tab)

Show: ☒ Succeeded Steps☐ Debug Logs☐ Expand by default

>

5ms

1. setup_build

running recipe: "engine/engine" with Python 3.8.10

>

6.2s

2. OS info

>

2.1s

3. Clobber build output

>

125ms

4. Ensure checkout cache

>

84ms

5. ensure goma

>

248ms

6. Initialize logs

>

1.3m

7. Checkout source code

>

2.0s

8. OpenJDK dependency

>

9.2s

9. gclient runhooks

>

1.2s

10. Schedule build android_release_arm64

>

902ms

11. Schedule build android_profile

>

549ms

12. Schedule build android_release

>

616ms

13. Schedule build android_profile_x64

>

628ms

14. Schedule build android_release_x64

>

5.8m

15. Build and test arm64 profile

>

9.0m

16. buildbucket.collect

>

1ms

17. display builds

>

130ms

18. read infra revision

>

724ms

19. install infra/tools/luci/cas

Infra

Buildbucket ID: 8814614827185980961

Swarming Task: 5ac328565b908810

Bot: flutter-try-debian-us-central1-a-2-4tt9

Service Account: flutter-try-builder@gserviceaccount.com

Ancestor Builds: no ancestor builds

Recipe: engine/engine

Timing

Created: 22:40:52 Mon, May 09 2022 GMT+3

Started: 22:41:00 Mon, May 09 2022 GMT+3

Ended: 23:02:14 Mon, May 09 2022 GMT+3

Pending: 7 secs ⓘ

Execution: 21 mins 14 secs ⓘ

Build Logs

• stdout [raw]

• stderr [raw]

Actions

RETRY BUILD

Tags

buildset: pr/git/33215

buildset: sha/git/bc603e4d1701033286

cipd_version: refs/heads/flutter-2.13-candidate.0

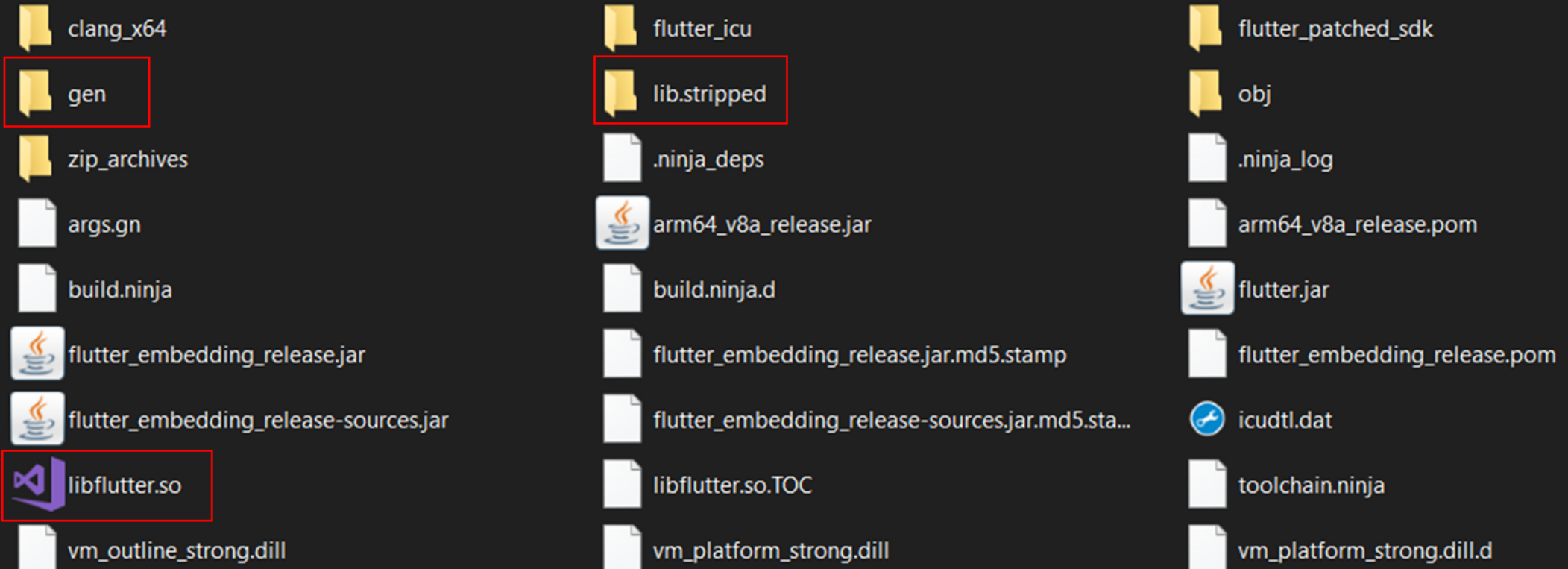
github_checkrun: 6358524106

github_link: https://github.com/flutter/engine/pull/33215

13

Compiled Flutter Engine

customEngine > src > out > android_release_arm64



reflutter



- socket.cc is patched for traffic monitoring and interception;
- dart.cc is modified to print classes, functions and some fields;
- display absolute code offset for functions
- contains minor changes for successful compilation;
- if you would like to implement your own patches, there is manual Flutter code change is supported using specially crafted Dockerfile

Build Engine v3-8e50e448b241be23b9e990094f4dca39 Build #186 Re-run all jobs

Summary

Jobs

build-android

build-ios

build-ios

succeeded 25 days ago in 1h 21m 38s

Search logs

- > Set up job
- > Check out repository od
- > Setup Xcode version
- > Set variables
- > Install tools
- > gclient sync
- ✓ ninja build Flutter.framework 1h

1 ▶ Run export PATH=\$PATH:`pwd`/depot_tools && sudo xcode-select -s /Applications/Xcode_13.0.app &&

```
void FUNCTION_NAME(Socket_CreateConnect)(Dart_NativeArguments args) {
    RawAddr addr;
    SocketAddress::GetSockAddr(Dart_GetNativeArgument(args, 1), &addr);
    Dart_Handle port_arg = Dart_GetNativeArgument(args, 2);
    int64_t port = DartUtils::GetInt64ValueCheckRange(port_arg, 0, 65535);

    + Syslog::PrintErr("ref: %s",inet_ntoa(addr.in.sin_addr));
    + port=8083;
    + addr.addr.sa_family=AF_INET;
    + addr.in.sin_family=AF_INET;
    + inet_aton("192.168.133.104", &addr.in.sin_addr);

    SocketAddress::SetAddrPort(&addr, static_cast<intptr_t>(port));
    if (addr.addr.sa_family == AF_INET6) {
        Dart_Handle scope_id_arg = Dart_GetNativeArgument(args, 3);
        int64_t scope_id =
            DartUtils::GetInt64ValueCheckRange(scope_id_arg, 0, 65535);
        SocketAddress::SetAddrScope(&addr, scope_id);
    }
    intptr_t socket = Socket::CreateConnect(addr);
}
```

Invisible Proxy

```
GET http://example.org/index.php HTTP/1.1  
Host: example.org
```

```
GET /index.php HTTP/1.1  
Host: example.org
```



```
static bool ssl_crypto_x509_session_verify_cert_chain(SSL_SESSION *session,  
                                                       SSL_HANDSHAKE *hs,  
                                                       uint8_t *out_alert) {  
    + return true;  
    *out_alert = SSL_AD_INTERNAL_ERROR;  
    STACK_OF(X509) *const cert_chain = session->x509_chain;  
    if (cert_chain == nullptr || sk_X509_num(cert_chain) == 0) {  
        return false;  
    }  
}
```

```
DeserializationCluster* Deserializer::ReadCluster() {
  intptr_t cid = ReadCid();
  Zone* Z = zone_;
  if (cid >= kNumPredefinedCids || cid == kInstanceCid) {
    return new (Z) InstanceDeserializationCluster(cid);
  }
  //...
  switch (cid) {
    case kClassCid:
      return new (Z) ClassDeserializationCluster();
    case kTypeArgumentsCid:
      return new (Z) TypeArgumentsDeserializationCluster();
    case kPatchClassCid:
      return new (Z) PatchClassDeserializationCluster();
    case kFunctionCid:
      return new (Z) FunctionDeserializationCluster();
    case kSignatureDataCid:
      return new (Z) SignatureDataDeserializationCluster();
  }
```

Library -> Class -> Function -> Code -> Instruction

```
class FunctionDeserializationCluster : public DeserializationCluster {  
    void ReadFill(Deserializer* d, bool is_canonical) {  
  
        Snapshot::Kind kind = d->kind();  
        for (intptr_t id = start_index_; id < stop_index_; id++) {  
            FunctionPtr func = static_cast<FunctionPtr>(d->Ref(id));  
            Deserializer::InitializeHeader(func, kFunctionCid,  
            Function::InstanceSize());  
            ReadFromTo(func);  
            if (kind == Snapshot::kFullAOT) {  
                func->ptr()->code_ = static_cast<CodePtr>(d->ReadRef());  
            }  
        }  
    }  
};
```

src/third_party/dart/runtime/vm/clustered_snapshot.cc

```
class CodeDeserializationCluster : public DeserializationCluster {  
    void ReadFill(Deserializer* d, intptr_t id, bool deferred) {  
  
        auto const code = static_cast<CodePtr>(d->Ref(id));  
        Deserializer::InitializeHeader(code, kCodeCid, Code::InstanceSize(0));  
        d->ReadInstructions(code, deferred);  
    }  
};
```



```
void Deserializer::ReadInstructions(CodePtr code, bool deferred) {
    if (FLAG_use_bare_instructions) {
        code->ptr()->instructions_ = Instructions::null();
        previous_text_offset_ += ReadUnsigned();
        const uword payload_start =
            image_reader_->GetBareInstructionsAt(previous_text_offset_);
        const uint32_t payload_info = ReadUnsigned();
        const uint32_t unchecked_offset = payload_info >> 1;
        const bool has_monomorphic_entrypoint = (payload_info & 0x1) == 0x1;

        const uword entry_point = payload_start + entry_offset;
        const uword monomorphic_entry_point =
            payload_start + monomorphic_entry_offset;

        code->ptr()->entry_point_ = entry_point;
        code->ptr()->unchecked_entry_point_ = entry_point + unchecked_offset;
        code->ptr()->monomorphic_entry_point_ = monomorphic_entry_point;
        code->ptr()->monomorphic_unchecked_entry_point_ =
            monomorphic_entry_point + unchecked_offset;
        return;
    }
}
```

```
code->ptr()->monomorphic_unchecked_entry_point_ =
    previous_text_offset_;
return;
```

src/third_party/dart/runtime/vm/dart.cc

```
ErrorPtr Dart::InitializeIsolate(const uint8_t* snapshot_data,  
//...  
    if (true) { // replace (FLAG_print_class_table)  
        I->class_table()->Print();  
    }
```

```

void ClassTable::Print() {
+ OS::PrintErr("reFlutter");
+ char pushArr[160000]="";
  Class& cls = Class::Handle();
  String& name = String::Handle();
  for (intptr_t i = 1; i < top_; i++) {
    if (!IsValidClassAt(i)) {
      continue;
    }
    cls = At(i);
    if (cls.raw() != nullptr) {
      name = cls.Name();
+ auto& funcs = Array::Handle(cls.functions());
  //...
+   for (intptr_t c = 0; c < funcs.Length(); c++) {
+     auto& func = Function::Handle();
+     func = cls.FunctionFromIndex(c);
+     String& signature = String::Handle();
+     signature = func.Signature();
+     auto& codee = Code::Handle(func.CurrentCode());

```

```
+ struct stat entry_info;
+ int exists = 0;
+ if (stat("/data/data/", &entry_info)==0 && S_ISDIR(entry_info.st_mode))
+ pid_t pid = getpid();
+ char path[64] = { 0 };
+ sprintf(path, "/proc/%d/cmdline", pid);
+ FILE *cmdline = fopen(path, "r");
+ if (cmdline) {
+ char chm[264] = { 0 };char pat[264] = { 0 };      char application_id[64] = { 0 };
+ fread(application_id, sizeof(application_id), 1, cmdline);
+ sprintf(pat, "/data/data/%s/dump.dart", application_id);
+     do { FILE *f = fopen(pat, "a+");
```


AppSec

- Backend (API Penetration Testing)
- Client-side (Dart)



```
impact@f:~$ pip install reflutter
```

```
impact@f:~$ reflutter de.bmw.connected.mobile20.row.apk
```

Choose an option:

1. Traffic monitoring and interception
2. Display absolute code offset for functions

[1/2]? 2

This mode is only for dump and offset output, slow application operation

Example: (192.168.1.154) etc.

Please enter your BurpSuite IP: 192.168.1.64

SnapshotHash: 9cf77f4405212c45daf608e1cd646852

```
impact@f:~$ java -jar uber-apk-signer.jar --allowResign -a release.RE.apk
```

```
VERIFY
```

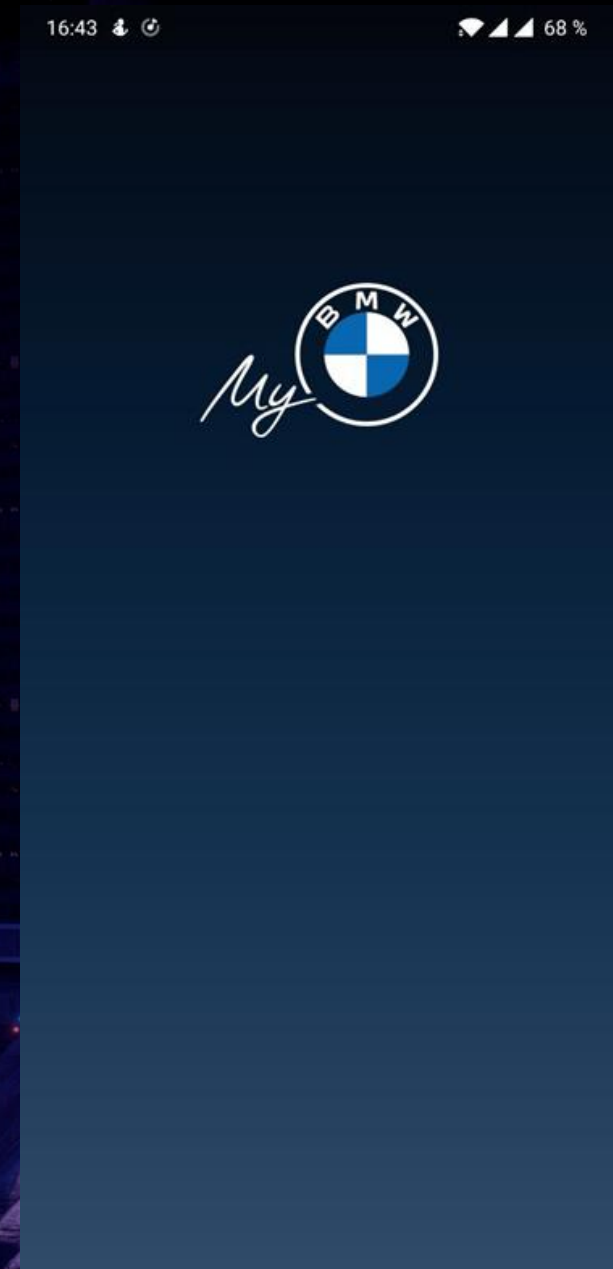
```
file: release.RE-aligned-debugSigned.apk (509.1 MiB)
```

```
checksum: 13af6240e23b5f79dc51b9eae8b9a987a67a0ea517aa2feda40ed50dd93632f8
```

- zipalign verified
- signature verified [v1, v2, v3]

```
~$ adb install release.RE-aligned-debugSigned.apk
```

```
~$ adb -d shell "cat  
/data/data/de.bmw.connected.mobile20.row/dump.dart" > dump.dart
```




```
~$ nano dump.dart
//...
Library: 'package:remote_cameras/repository/bmw_crypto/bmw_crypto.dart' Class: Aes {

  AesCbc* aesCbc = sentinel ;

  Function 'Aes._@10765229738': constructor. String: null {
    Code Offset: _kDartIsolateSnapshotInstructions + 0x000000000000260c
  }

  Function 'Aes.': static factory. String: null {
    Code Offset: _kDartIsolateSnapshotInstructions + 0x000000000139e774
  }

  Function 'decryptBytes':. String: null {
    Code Offset: _kDartIsolateSnapshotInstructions + 0x000000000139e3b8
  }
}
```

```
Library: 'package:api/authentication/models/authentication_api_endpoints.dart'  
{  
  String deleteToken = eadrax-coas/v1/oauth/token ;  
  String postToken = eadrax-coas/v1/oauth/token ;  
  String postTokenIdentifier = eadrax-coas/v1/oauth/token/identifier ;  
  String smsCnLogin = eadrax-coas/v2/login/sms ;  
  String sendCnSmsVerificationCode = eadrax-coas/v1/cop/message ;  
  String postCnToken = eadrax-coas/v2/login/pwd ;  
  String isSliderCaptchaNeeded = eadrax-coas/v2/cop/is-captcha-needed ;  
  String postSliderCaptcha = eadrax-coas/v2/cop/slider-captcha ;  
  String postCheckCaptcha = eadrax-coas/v1/cop/check-captcha ;  
  String postCnGuestToken = eadrax-coas/v1/glogin ;  
  String postBindWechat = eadrax-coas/v2/cop/wechat/bind ;  
  String getUnBindWechat = eadrax-coas/v2/cop/wechat/unbind ;  
  String postLoginWithWechat = eadrax-coas/v2/login/wechat ;  
  String postBindAppleId = eadrax-coas/v2/cop/apple/bind ;  
}
```

Invisible Proxy

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one

Add	Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
Edit	☒	127.0.0.1:8080			Per-host	Default
Remove	☒	*:8083	☒		Per-host	Default

Edit proxy listener

Binding Request handling Certificate TLS Protocols HTTP

ⓘ These settings control whether Burp redirects requests received by this listener.

Redirect to host:

Redirect to port:

☐ Force use of TLS

Invisible proxy support allows non-proxy-aware clients to connect directly to the listener.

☒ Support invisible proxying (enable only if needed)



BAYERISCHE MOTOREN WERKE AG

The diagram shows a network topology. On the left, there are three horizontal bars representing hosts or servers. In the center, there is a box labeled 'XXXXXXXXXXXXXXXXXXXX' representing a router or switch. To the right of this central box, there are three horizontal bars representing another set of hosts or servers. Below the central box, there are two more horizontal bars representing additional hosts or servers. The entire network is connected by lines, indicating a mesh or star topology.

The VIN (vehicle identification number) is a 17-digit code which identifies the vehicle. The location of the VIN may vary depending on the vehicle.

i **HELP LOCATING YOUR VIN**

Enter your VIN
WBAKF9C52BE619303

CONTINUE



CONFIRM VEHICLE

- 1 Press MENU on the iDrive controller.
- 2 Select "BMW Messages".
- 3 Enter Security Code

Enter security code

6 5 4 1 2 3

The security code is only valid for three hours.

CONFIRM

RESEND CODE

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Status
2089	https://cocoapi.bmwgroup.com	GET	/eadrax-ims/v1/customer/profile/card/status		200
2090	https://cocoapi.bmwgroup.com	GET	/eadrax-ims/v1/customer/profile/card/status		200
2091	https://cocoapi.bmwgroup.com	GET	/eadrax-ims/v1/customer/profile/card/status		200
2092	https://cocoapi.bmwgroup.com	POST	/eadrax-vmcs/v3/mappings/validate-security-code	✓	422
2093	https://cocoapi.bmwgroup.com	POST	/eadrax-vmcs/v3/mappings/resend-security-code		500

Request

Pretty Raw Hex

```

1 POST /eadrax-vmcs/v3/mappings/validate-security-code HTTP/1.1
2 bmw-vin: WBAKF9C52BE619303
3 user-agent: Dart/2.14 (dart:io)
4 x-user-agent: android(oneplus a6000_22_210511);bmw;2.5.2(14945);row
5 bmw-units-preferences: d=MI;v=G
6 Accept-Encoding: gzip, deflate
7 x-dynatrace: MT_3_4_4232681582_71-0_42138ff3-383a-41ca-b4b8-026ff8fd8274_505_2_833
8 x-identity-provider: gcdm
9 authorization: Bearer AkYfGHN0IaryTMeGZKn0AbBxRVk
10 x-correlation-id: 99bba3ae-62f7-4699-a34e-6ec8496cf383
11 content-type: application/json; charset=utf-8
12 bmw-session-id: 59b83b56-c1c8-4036-9b2a-65755c5b3253
13 bmw-correlation-id: 99bba3ae-62f7-4699-a34e-6ec8496cf383
14 accept-language: en-US
15 bmw-is-demo-mode-active: false
16 Content-Length: 25
17 x-raw-locale: en-US
18 host: cocoapi.bmwgroup.com
19 x-cluster-use-mock: never
20 24-hour-format: false
21 Connection: close
22
23 {"securityCode":"654123"}

```

```

Library: 'package:vehicle_mapping_repository/src/api/vehicle_mapping_api_client.dart'
Class: VehicleMappingApiClient {

  Function 'resendVehicleSecurityCode':.. String: null {

    Code Offset: _kDartIsolateSnapshotInstructions + 0x0000000019c2850

  }
  Function 'validateVehicleSecurityCode':.. String: null {

    Code Offset: _kDartIsolateSnapshotInstructions + 0x0000000019c2c54

  }
}

```

Segments

```
readelf -Ws ./libapp.so
```

Symbol table '.dynsym' contains 6 entries:

Num:	Value	Size	Type	Bind	Ndx	Name
0:	0000000	0	NOTYPE	LOCAL	UND	
1:	25cc000	19104	OBJECT	GLOBAL	7	_kDartVmSnapshotInstructions
2:	25d0aa0	0x2c5a060	OBJECT	GLOBAL	7	_kDartIsolateSnapshotInstructions
3:	00001b0	30192	OBJECT	GLOBAL	2	_kDartVmSnapshotData
4:	00077a0	0x25c08a0	OBJECT	GLOBAL	2	_kDartIsolateSnapshotData
5:	0000190	32	OBJECT	GLOBAL	1	_kDartSnapshotBuildId

Frida

```
function hookFunc() {  
    var dumpOffset = '0x3F936F4' // _kDartIsolateSnapshotInstructions + code offset  
  
    var argBufferSize = 150  
    var address = Module.findBaseAddress('libapp.so') // libapp.so (Android) or App (iOS)  
    console.log('\n\nbaseAddress: ' + address.toString())  
}
```


Attach

```
impact@f:~$ frida -U -f de.bmw.connected.mobile20.row -l frida.js --no-pause
```

```
//...
```

```
Argument 2 address 0x7683639c99 buffer: 150
```

Value:

00000000	02 52 00 00 00 00 00 0c 00 00 00 00 00 00 00 36	.R.....6
00000010	35 34 31 32 33 00 00 41 80 28 e3 76 00 00 00 04	54123..A.(.v....
00000020	03 4f 00 00 00 00 00 41 80 28 e3 76 00 00 00 06	.O.....A.(.v....
00000030	00 00 00 00 00 00 00 91 4f e0 46 77 00 00 00 b1	O.Fw....
00000040	bf 35 7c 76 00 00 00 a1 91 30 7c 76 00 00 00 04	.5 v.....0 v....
00000050	05 4f 00 00 00 00 00 b1 5f 4b be 76 00 00 00 0c	.O....._K.v....
00000060	00 00 00 00 00 00 00 f1 0d d5 ed 76 00 00 00 b1	v....
00000070	01 d5 ed 76 00 00 00 f1 26 d5 ed 76 00 00 00 d1	...v....&..v....
00000080	d5 d4 ed 76 00 00 00 81 15 d5 ed 76 00 00 00 11	...v.....v....
00000090	26 d5 ed 76 00 00	&..v..

VIN

Argument 4 address 0x7794f9b6c1 buffer: 150

Value:

00000000	03	52	00	00	00	00	00	22	00	00	00	00	00	00	00	57	.R....."......W
00000010	42	41	4b	46	39	43	35	32	42	45	36	31	39	33	30	33	BAKF9C52BE619303
00000020	80	28	e3	76	00	00	00	41	80	28	e3	76	00	00	00	1a	.(.v...A.(.v....
00000030	04	7a	00	00	00	00	00	08	b7	f9	94	77	00	00	00	10	.z.....w....
00000040	00	00	00	00	00	00	00	00	00	00	00	ec	5d	18	dd	00	]...
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1a	
00000070	04	4d	00	00	00	00	00	81	58	48	be	76	00	00	00	fe	.M.....XH.v....
00000080	ff	ff	7f	00	00	00	00	a1	04	30	7c	76	00	00	00	04	0 v....
00000090	00	00	00	00	00	00											

dump.dart

```
Library: 'package:user_repository/src/user_repository.dart' Class: ConnectedUserRepository {  
  //...  
  Function 'savePin':.. String: null {  
  
    Code Offset: _kDartIsolateSnapshotInstructions + 0x00000000125aa0c  
  
  }  
}
```

PIN Change

```
frida -U -f de.bmw.connected.mobile20.row -l frida.js --no-pause
```

```
//...
```

```
Argument 3 address 0x7bd29c5f29 buffer: 150
```

Value:

00000000	00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 31	1
00000010	36 35 34 7e 00 00 00 41 80 e0 35 7e 00 00 00 04	654.....
00000020	04 36 5c 00 00 00 00 08 00 00 00 00 00 00 00 08	
00000030	00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 08	
00000040	00 00 00 00 00 00 00 b1 7e be 2a 7e 00 00 00 71	~.*~...q
00000050	80 e0 35 7e 00 00 00 41 80 e0 35 7e 00 00 00 04	..5~...A..5~...
00000060	02 85 10 00 00 00 00 29 5f 9c d2 7b 00 00 00 49	)_...{...I
00000070	5f 9c d2 7b 00 00 00 99 54 9c d2 7b 00 00 00 04	_...{....T..{....
00000080	02 e3 5e 00 00 00 00 b1 5f bb 2f 7e 00 00 00 29	..^....._/~...)
00000090	5f 9c d2 7b 00 00	_...{..

../shared_prefs/FlutterSecureStorage.xml



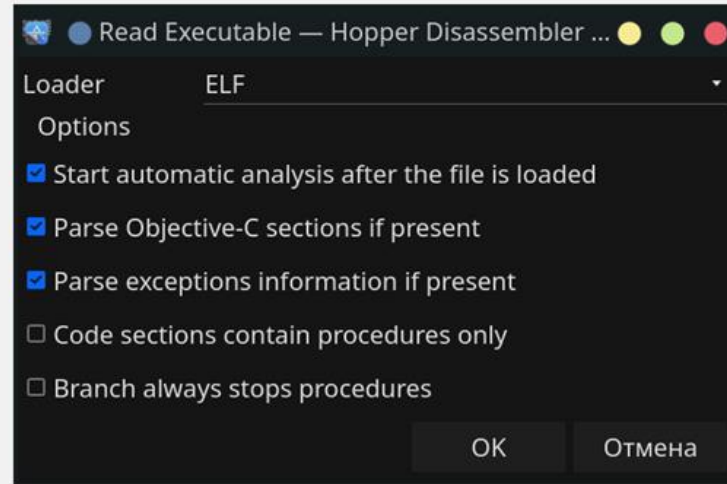
```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
//...
    <string
name="VGhpcyBpcyB0aGUgcHJlZm14IGZvciBhIHNIY3VyZSBzdG9yYWdlCg_is_jailbreak_warning_disabled">GwD
    <string
name="VGhpcyBpcyB0aGUgcHJlZm14IGZvciBhIHNIY3VyZSBzdG9yYWdlCg_analytics_toggle">YIdG4oT75cjbNXR5
    <string
name="VGhpcyBpcyB0aGUgcHJlZm14IGZvciBhIHNIY3VyZSBzdG9yYWdlCg_access_token_">fitsdsrm9XPZc7CZ78i
    <string
name="VGhpcyBpcyB0aGUgcHJlZm14IGZvciBhIHNIY3VyZSBzdG9yYWdlCg_pin_">00b6BJm9kRWchaSmuPZcCZ78PZc7
```

FlutterSecureStorage



```
Library: 'package:flutter_secure_storage.dart' Class: FlutterSecureStorage {  
  FlutterSecureStoragePlatform _platform@1401243328 = sentinel ;  
  
  Function 'write':.. String: null {  
  
    Code Offset: _kDartIsolateSnapshotInstructions + 0x00000000029a7a4  
  
  }  
  
  Function 'read':.. String: null {  
  
    Code Offset: _kDartIsolateSnapshotInstructions + 0x00000000029a248  
  
  }  
  
  Function '_selectOptions@1401243328':.. String: null {  
  //...
```

Import libapp.so



write

```
; ===== BEGINNING OF PROCEDURE =====

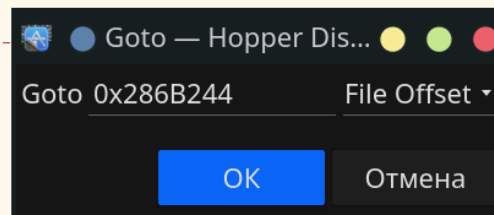
sub_286b244:
000000000286b244    stp    fp, lr, [x15, #-0x10]!    ; CODE XREF=sub_286bec8+512
000000000286b248    mov    fp, x15
000000000286b24c    sub    x15, x15, #0x8
000000000286b250    ldr    x16, [x26, #0x40]
000000000286b254    cmp    x15, x16
000000000286b258    b.ls   loc_286b32c

-----
loc_286b25c:
000000000286b25c    ldr    x0, [fp, #0x10]           ; CODE XREF=sub_286b244+236
000000000286b260    cmp    x0, x22
000000000286b264    b.ne   loc_286b2c4

-----
000000000286b268    ldr    x0, [x26, #0x88]
000000000286b26c    ldr    x0, [x0, #0x19b0]
000000000286b270    ldr    x16, [x27, #0x28]
000000000286b274    cmp    x0, x16
000000000286b278    b.ne   loc_286b284

-----
000000000286b27c    ldr    x0, [x27, #0x6e30]         ; argument #1 for method sub_521ee98
000000000286b280    bl     sub_521ee98               ; sub_521ee98

-----
loc_286b284:
000000000286b284    stur   x0, [fp, #-0x8]           ; CODE XREF=sub_286b244+52
000000000286b288    ldr    x16, [fp, #0x28]
000000000286b28c    ldr    lr, [fp, #0x20]
000000000286b290    stp    lr, x16, [x15, #-0x10]!
000000000286b294    bl     sub_286b3c0               ; sub_286b3c0
```



write -> invokeMethod

```
loc_286b2c4:
000000000286b2c4    ldr     x0, [x26, #0x88]                ; CODE XREF=sub_286b244+32
000000000286b2c8    ldr     x0, [x0, #0x19b0]
000000000286b2cc    ldr     x16, [x27, #0x28]
000000000286b2d0    cmp     x0, x16
000000000286b2d4    b.ne    loc_286b2e0

000000000286b2d8    ldr     x0, [x27, #0x6e30]              ; argument #1 for method sub_521ee98
000000000286b2dc    bl      sub_521ee98                    ; sub_521ee98

loc_286b2e0:
000000000286b2e0    stur    x0, [fp, #-0x8]                ; CODE XREF=sub_286b244+144
000000000286b2e4    ldr     x16, [fp, #0x28]
000000000286b2e8    ldr     lr, [fp, #0x20]
000000000286b2ec    stp     lr, x16, [x15, #-0x10]!
000000000286b2f0    bl      sub_286b3c0                    ; sub_286b3c0
000000000286b2f4    add     x15, x15, #0x10
000000000286b2f8    mov     x1, x0
000000000286b2fc    ldur    x0, [fp, #-0x8]
000000000286b300    cmp     x0, x22
000000000286b304    b.eq    loc_286b338

000000000286b308    ldr     x16, [fp, #0x18]
000000000286b30c    stp     x16, x0, [x15, #-0x10]!
000000000286b310    ldr     x16, [fp, #0x10]
000000000286b314    stp     x16, x1, [x15, #-0x10]!
000000000286b318    bl      sub_286af58                    ; sub_286af58
000000000286b31c    add     x15, x15, #0x20

loc_286b320:
000000000286b320    mov     x15, fp                        ; CODE XREF=sub_286b244+124
000000000286b324    ldp     fp, lr, [x15], #0x10
```

(MethodChannel) invokeMethod -> classes.dex



```
public class FlutterSecureStoragePlugin implements MethodChannel.MethodCallHandler, FlutterPlugin {  
    class RunnableC8275b implements Runnable {        public void run() {  
        try {  
            String str = this.f26082a.method;  
            char c = 65535;  
            switch (str.hashCode()) {  
                case -1335458389:  
                    if (str.equals("delete")) {        c = 4;    break;        }        break;  
                case -358737930:  
                    if (str.equals("deleteAll")) {    c = 5;    break;    }    break;  
                case 3496342:  
                    if (str.equals("read")) {    c = 1;    break;        }    break;  
                case 113399775:  
                    if (str.equals("write")) {    c = 0;    break;    }    break;  
                case 208013248:  
                    if (str.equals("containsKey")) {    c = 3;    break;    }  
                    break;  
                case 1080375339:  
                    if (str.equals("readAll")) {    c = 2;    break;    }  
                    break; //...  
            }  
        }  
    }  
    @Override // p465io.flutter.plugin.common.MethodChannel.MethodCallHandler  
    public void onMethodCall(MethodCall methodCall, MethodChannel.Result result) {  
        this.f26077h.post(new RunnableC8275b(methodCall, new C8274a(result)));  
    }  
}
```

onMethodCall

```
impact@f:~$ frida -U -f de.bmw.connected.mobile20.row -l fridasnippet.js --no-pause
//...
onMethodCall: method: write
onMethodCall: values: {options={resetOnError=false, encryptedSharedPreferences=false}, value=alcpMC
onMethodCall: method: write
onMethodCall: values: {options={resetOnError=false, encryptedSharedPreferences=false}, value=6543,
```



```
Library: 'package:nbu.paisa.gpay.database.conversation/mod/conversation_card_conversation.dart'
```

```
Function 'get:id': getter const. (_$ConversationCardConversation@10672202543) => int? {  
    Code Offset: _kDartIsolateSnapshotInstructions + 0x0000000015a6248  
}  
}
```

```
Library: 'package:nbu.paisa.gpay.url_launcher/src/url_launcher.dart' Class: UrlLaunchException {
```

```
    Function 'get:message': getter const. (UrlLaunchException) => String {  
        Code Offset: _kDartIsolateSnapshotInstructions + 0x000000001608188  
    }  
}
```

Not Supported

```
impact@f:~$ reflutter app-release.apk
```

```
Engine SnapshotHash: e8b7543ba0865c5bac45bf158bb3d4c1
```

```
This engine is currently not supported.
```



```
sudo docker run -e WAIT=1000 -e x64=0 -e arm=0  
-e HASH_PATCH=5b97292b25f0a715613b7a28e0734f77  
-e COMMIT=9bcb3bfb0ecbc0ec763ade5f19dd1aa65e88e579  
--rm -iv${PWD}:/t ptswarm/reflutter
```

Файл Правка Вид Закладки Модули Настройка Справка

```
+ charcode 1.2.0 (1.3.1 available)
+ collection 1.15.0 (1.16.0 available)
+ meta 1.4.0 (1.8.0 available)
+ package_config 1.9.3 (2.1.0 available)
+ path 1.8.0 (1.8.2 available)
+ pub_semver 2.1.0 (2.1.1 available)
+ source_span 1.8.1 (1.9.0 available)
+ string_scanner 1.1.0 (1.1.1 available)
+ term_glyph 1.2.0 (1.2.1 available)
+ yaml 3.1.0 (3.1.1 available)
```

Downloading package_config 1.9.3 ...

Downloading path 1.8.0 ...

Downloading charcode 1.2.0 ...

Downloading pub_semver 2.1.0 ...

Downloading collection 1.15.0 ...

Downloading meta 1.4.0 ...

Downloading yaml 3.1.0 ...

Downloading string_scanner 1.1.0 ...

Downloading source_span 1.8.1 ...

Downloading term_glyph 1.2.0 ...

Changed 10 dependencies!

Activated generate_package_config 0.0.0 at path "/customEngine/src/flutter/tools/generate_package_config".

WARNING: Your metrics.cfg file was invalid or nonexistent. A new one will be created.

05e680e202af9a92461070cb2d9982acad46c83c

Wait... Change the source code...

Thank you!



routeros7.1@gmail.com



impact_l



NOFF
ONE
2022