com.apksonar.demo.criticaldeep

demo-criticaldeep-aligned-debugSigned.apk · SHA-256 24c27326f556d94e… · deep scan · finished 2026-11-18T19:48:55 UTC

CRITICAL × 32 | HIGH × 28 | MEDIUM × 3 | 83 secret families | OWASP MASVS | CVSS 3.1

OWASP MASVS: STORAGE · CODE · RESILIENCE · CRYPTO

APPLICATION

version 1.0 (1) · SDK 24→35 · 16.8 KB · 12 files · 1 dex

FINDINGS · 63

Stripe live secret key

classes.dex

sk_li••••0001 · 34 chars

secrets · MASVS-STORAGE · CVSS 9.1

Stripe live secret key

classes.dex

sk_li••••0002 · 34 chars

secrets · MASVS-STORAGE · CVSS 9.1

AWS access key id

classes.dex

AKIA•••• · 20 chars

secrets · MASVS-STORAGE · CVSS 9.1

AWS access key id

classes.dex

AKIA•••• · 20 chars

secrets · MASVS-STORAGE · CVSS 9.1

Private key block

classes.dex

OPENSSH PRIVATE KEY (только заголовок, тело вне корпуса сканирования)

secrets · MASVS-STORAGE · CVSS 9.1

OpenAI API key

classes.dex

sk-pr••••00AA · 48 chars

secrets · MASVS-STORAGE · CVSS 9.1

Anthropic API key

classes.dex

sk-an••••00AA · 45 chars

secrets · MASVS-STORAGE · CVSS 9.1

xAI (Grok) API key

classes.dex

xai-C••••0000 · 39 chars

secrets · MASVS-STORAGE · CVSS 9.1

GitHub personal access token

classes.dex

ghp_C••••oApk · 40 chars

secrets · MASVS-STORAGE · CVSS 9.1

Square access token

classes.dex

sak_C••••calD · 34 chars

secrets · MASVS-STORAGE · CVSS 9.1

Braintree production token

classes.dex

acces••••ical · 65 chars

secrets · MASVS-STORAGE · CVSS 9.1

DigitalOcean API token

classes.dex

dop_v••••ffee · 71 chars

secrets · MASVS-STORAGE · CVSS 9.1

Cloudflare global API key — classes.dex
cloud••••1234 · 56 chars
secrets · MASVS-STORAGE · CVSS 9.1

GitLab personal access token — classes.dex
glpat••••en00 · 33 chars
secrets · MASVS-STORAGE · CVSS 9.1

GitHub OAuth token — classes.dex
gho_C••••oApk · 40 chars
secrets · MASVS-STORAGE · CVSS 9.1

GitHub user token — classes.dex
ghu_C••••oApk · 40 chars
secrets · MASVS-STORAGE · CVSS 9.1

GitHub server token — classes.dex
ghs_C••••oApk · 40 chars
secrets · MASVS-STORAGE · CVSS 9.1

GitHub refresh token — classes.dex
ghr_C••••oApk · 40 chars
secrets · MASVS-STORAGE · CVSS 9.1

GitHub fine-grained token — classes.dex
githu••••ical · 61 chars
secrets · MASVS-STORAGE · CVSS 9.1

OpenRouter API key — classes.dex
sk-or••••cafe · 73 chars
secrets · MASVS-STORAGE · CVSS 9.1

Perplexity API key — classes.dex
pplx-••••ffee · 53 chars
secrets · MASVS-STORAGE · CVSS 9.1

Hugging Face token — classes.dex
hf_Cr••••e000 · 37 chars
secrets · MASVS-STORAGE · CVSS 9.1

Shopify access token — classes.dex
shpat••••0c0f · 38 chars
secrets · MASVS-STORAGE · CVSS 9.1

Shopify access token — classes.dex
shpca••••0c0f · 38 chars
secrets · MASVS-STORAGE · CVSS 9.1

Razorpay live key id — classes.dex
rzp_•••• · 23 chars
secrets · MASVS-STORAGE · CVSS 9.1

Flutterwave live secret — classes.dex
FLWSE••••e000 · 34 chars
secrets · MASVS-STORAGE · CVSS 9.1

AWS secret access key — classes.dex
aws_s••••emoA · 64 chars
secrets · MASVS-STORAGE · CVSS 9.1

GitLab group token — classes.dex
glptt••••upT0 · 33 chars
secrets · MASVS-STORAGE · CVSS 9.1

Stripe live secret key — assets/config.json
sk_li••••0001 · 37 chars
secrets · MASVS-STORAGE · CVSS 9.1

Private key block — assets/config.json
RSA PRIVATE KEY (только заголовок, тело вне корпуса сканирования)
secrets · MASVS-STORAGE · CVSS 9.1

OpenAI API key — assets/config.json
sk-pr••••00AA · 45 chars
secrets · MASVS-STORAGE · CVSS 9.1

Private key embedded in JSON config — assets/config.json
priva••••EGIN · 25 chars
secrets · MASVS-STORAGE · CVSS 9.1

Groq API key — classes.dex
gsk_C••••0000 · 39 chars
secrets · MASVS-STORAGE · CVSS 8.2

Slack bot token — classes.dex
xoxb-••••0000 · 52 chars
secrets · MASVS-STORAGE · CVSS 8.2

Telegram bot token — classes.dex
12345••••gram · 46 chars
secrets · MASVS-STORAGE · CVSS 8.2

SendGrid API key — classes.dex
SG.Cr••••0000 · 69 chars
secrets · MASVS-STORAGE · CVSS 8.2

Google OAuth client secret — classes.dex
GOCSP••••cret · 37 chars
secrets · MASVS-STORAGE · CVSS 8.2

Google OAuth refresh token — classes.dex
1//0C••••0000 · 45 chars
secrets · MASVS-STORAGE · CVSS 8.2

Azure storage account key — classes.dex
Accou••••ng== · 68 chars
secrets · MASVS-STORAGE · CVSS 8.2

Linode API key — classes.dex
linod••••Crit · 51 chars
secrets · MASVS-STORAGE · CVSS 8.2

Cloudflare API token — classes.dex
cloud••••oudf · 61 chars
secrets · MASVS-STORAGE · CVSS 8.2

Firebase (FCM) legacy server key — classes.dex
AAAAC••••calD · 40 chars
secrets · MASVS-STORAGE · CVSS 8.2

Twilio API key — classes.dex
SK000••••0ffe · 34 chars
secrets · MASVS-STORAGE · CVSS 8.2

Twilio API key — classes.dex
SKc0f••••6789 · 34 chars
secrets · MASVS-STORAGE · CVSS 8.2

Mailgun API key — classes.dex
key-C••••emoM · 36 chars
secrets · MASVS-STORAGE · CVSS 8.2

Mailchimp API key — classes.dex
01234••••us19 · 37 chars
secrets · MASVS-STORAGE · CVSS 8.2

New Relic API key — classes.dex
NRAK-••••Reli · 32 chars
secrets · MASVS-STORAGE · CVSS 8.2

Live API key (MessageBird/YooKassa) — classes.dex
live_••••calD · 37 chars
secrets · MASVS-STORAGE · CVSS 8.2

Discord bot token — classes.dex
MTExM••••0000 · 62 chars
secrets · MASVS-STORAGE · CVSS 8.2

Discord webhook URL — classes.dex
https••••0000 · 100 chars
secrets · MASVS-STORAGE · CVSS 8.2

Slack webhook URL — classes.dex
hooks••••0000 · 81 chars
secrets · MASVS-STORAGE · CVSS 8.2

Facebook classic access token — classes.dex
EAACE••••B000 · 42 chars
secrets · MASVS-STORAGE · CVSS 8.2

Notion integration token — classes.dex
secre••••moNo · 50 chars
secrets · MASVS-STORAGE · CVSS 8.2

Linear API key — classes.dex
lin_a••••earK · 48 chars
secrets · MASVS-STORAGE · CVSS 8.2

Postman API key — classes.dex
PMAK-••••0000 · 47 chars
secrets · MASVS-STORAGE · CVSS 8.2

Sentry org auth token — classes.dex
sntry••••0000 · 41 chars
secrets · MASVS-STORAGE · CVSS 8.2

Credentials in database/service URL — classes.dex
postg••••ass@ · 31 chars
secrets · MASVS-STORAGE · CVSS 8.2

Password in JDBC URL

classes.dex

jdbc:••••o · 1006 chars

secrets · MASVS-STORAGE · CVSS 8.2

Google API key in code

res/values/strings.xml

AIzaC••••000A · 39 chars

secrets · MASVS-STORAGE · CVSS 8.2

Groq API key

res/values/strings.xml

gsk_C••••0000 · 39 chars

secrets · MASVS-STORAGE · CVSS 8.2

Signed with a debug certificate

C=US
ST=US
L=US
O=US
OU=Android
CN=Android Debug

The APK is signed with the Android Debug certificate. Debug builds must never ship: they can be trivially replaced and usually enable extra logging and debugging paths.

signing · MASVS-CODE · CVSS 4.8

Packed native library: libunity_demo.so

libunity_demo.so

UPX packer marker

The .so is packed with UPX. Packing hides the real code from static analysis and is common in obfuscated SDKs, cheats and malware loaders.

native · MASVS-RESILIENCE · CVSS 3.7

Outdated OpenSSL 1.0.2u statically linked in libcrypto_demo.so

libcrypto_demo.so

OpenSSL 1.0.2u

OpenSSL 1.0.x/1.1.x is EOL and carries known CVEs; it is compiled into the app, so updates depend on the app vendor, not the OS.

crypto · MASVS-CRYPTO · CVSS 7.4

PERMISSIONS · 12 (10 dangerous)

INTERNET · ACCESS_FINE_LOCATION · ACCESS_BACKGROUND_LOCATION · READ_CONTACTS · READ_SMS · RECEIVE_SMS · RECORD_AUDIO · CAMERA · READ_EXTERNAL_STORAGE · RECEIVE_BOOT_COMPLETED · CALL_PHONE · BLUETOOTH_SCAN

COMPONENTS · 2 activities · 1 services · 1 receivers · 1 providers · 5 exported

MainActivity · TrackingActivity · LocationSyncService · SmsReceiver · DataProvider

SDK INVENTORY · 5

Firebase (analytics/crash) · Facebook SDK (social/ads) · Amplitude (analytics) · OneSignal (push) · myTracker (analytics)

NATIVE LIBRARIES · 4

libapksonar_demo.so · x86_64 · 13.4 KB
libunity_demo.so · x86_64 · 13.4 KB · packer: UPX
libapksonar_demo.so · arm64-v8a · 0.1 KB
libcrypto_demo.so · arm64-v8a · 0.1 KB · 1.0.2u

NATIVE ANALYSIS · GHIDRA · 2 libs

libcrypto_demo.so · arm64-v8a · 0 procedures · 0 strings · 0.1 KB · entropy 2.3 · shared

libapksonar_demo.so · x86_64 · 1 procedures · 22 strings · 13.4 KB · entropy 0.59 · shared

Ghidra decompiler · apksonar_demo_marker

```
undefined8 apksonar_demo_marker(void)

{
return 0x2a;
}
```

JAVA ANALYSIS · JADX · 8 classes · obfuscation 0%

com.apksonar.demo.criticaldeep (2) · com.amplitude.api (1) · com.facebook.appevents (1) · com.google.firebase.analytics (1) · com.my.tracker (1) · com.onesignal (1)

No trust-all TLS hooks or JS-bridged WebViews flagged in decompiled code.

SIGNATURE

scheme: v3 · C=US
ST=US
L=US
O=US
OU=Android
CN=Android Debug · rsa
valid 2016-10-23 → 2044-03-10 · cert SHA-256 1e08a903aef9c3a7…