MOBSF

IOS STATIC ANALYSIS REPORT

BatteryDoctor

File Name:	BatteryDoctor 3.2.ipa
Identifier:	com.easysoft.BatteryDoctor
Scan Date:	Oct. 9, 2025, 6:44 a.m.
App Security Score:	24/100 (CRITICAL RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	1	1	1	0

FILE INFORMATION

File Name: BatteryDoctor 3.2.ipa
Size: 1.36MB
MD5: e3dc31591219960747719cbdebfd8c87
SHA1: c9f33e0d4f82167ed349ac4eb8a388ba29412fdc
SHA256: bcf1e4450d204df13dea9f2b7ab049d8dbce5dd7ab1d7b69ce0a2dea0cd44ff8

APP INFORMATION

App Name: BatteryDoctor
App Type: Objective C
Identifier: com.easysoft.BatteryDoctor
SDK Name: iphoneos3.0
Version:
Build: 3.2
Platform Version: 3.2
Min OS Version: 3.0
Supported Platforms: iPhoneOS,

BINARY INFORMATION

Arch: ARM
Sub Arch: CPU_SUBTYPE_ARM_V6
Bit: 32-bit
Endian: <

APP TRANSPORT SECURITY (ATS)

NO	ISSUE	SEVERITY	DESCRIPTION

IPA BINARY CODE ANALYSIS

HIGH: 2 | WARNING: 0 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	DESCRIPTION
1	Binary makes use of the insecure Random function(s)	high	**CWE:** CWE-330: Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6	The binary may use the following insecure Random function(s) _random
2	Binary makes use of Logging function	info	**CWE:** CWE-532: Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3	The binary may use _NSLog function for logging.
3	Binary makes use of malloc function	high	**CWE:** CWE-789: Uncontrolled Memory Allocation **OWASP Top 10:** M7: Client Code Quality **OWASP MASVS:** MSTG-CODE-8	The binary may use _malloc function instead of calloc

IPA BINARY ANALYSIS

PROTECTION	STATUS	SEVERITY	DESCRIPTION
NX	True	info	The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.
PIE	False	high	The binary is built without Position Independent Code flag. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack,heap and libraries. Use compiler option -fPIC to enable Position Independent Code. Not applicable for dylibs and static libraries.
STACK CANARY	False	high	This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.
ARC	False	high	The binary is not compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and protects from memory corruption vulnerabilities. Use compiler option -fobjc-arc to enable ARC or set Objective-C Automatic Reference Counting to YES in project configuration.
RPATH	False	info	The binary does not have Runpath Search Path (@rpath) set.
CODE SIGNATURE	True	info	This binary has a code signature.
ENCRYPTED	False	warning	This binary is not encrypted.
SYMBOLS STRIPPED	False	warning	Debug Symbols are available. To strip debugging symbols, set Strip Debug Symbols During Copy to YES, Deployment Postprocessing to YES, and Strip Linked Product to YES in project's build settings.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
arashpayan.com	ok	**IP:** 192.155.83.134 **Country:** United States of America **Region:** California **City:** Fremont **Latitude:** 37.548271 **Longitude:** -121.988571 **View:** Google Map
purl.org	ok	**IP:** 207.241.225.157 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.781734 **Longitude:** -122.459435 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
itunes.com	ok	**IP:** 17.253.144.11 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486

		View: Google Map
www.apple.com	ok	IP: 184.50.196.247 Country: Japan Region: Tokyo City: Tokyo Latitude: 35.689507 Longitude: 139.691696 View: Google Map
www.w3.org	ok	IP: 104.18.23.19 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

EMAILS

EMAIL	FILE
gamelingosupport@gmail.com	BatteryDoctor.app/Tips.html
gamelingosupport@gmail.com	BatteryDoctor.app/BatteryDoctor
gamelingosupport@gmail.com	IPA Strings Dump

SCAN LOGS

Timestamp	Event	Error

2025-10-09 06:44:42	iOS Binary (IPA) Analysis Started	OK
2025-10-09 06:44:42	Generating Hashes	OK
2025-10-09 06:44:42	Extracting IPA	OK
2025-10-09 06:44:42	Unzipping	OK
2025-10-09 06:44:42	iOS File Analysis and Normalization	OK
2025-10-09 06:44:42	iOS Info.plist Analysis Started	OK
2025-10-09 06:44:42	Finding Info.plist in iOS Binary	OK
2025-10-09 06:44:43	Fetching Details from App Store: com.easysoft.BatteryDoctor	OK
2025-10-09 06:44:44	Searching for secrets in plist files	OK
2025-10-09 06:44:44	Starting Binary Analysis	OK
2025-10-09 06:44:45	Dumping Classes from the binary	OK

2025-10-09 06:44:45	Running jtool against the binary for dumping classes	OK
2025-10-09 06:44:45	Library Binary Analysis Started	OK
2025-10-09 06:44:45	Framework Binary Analysis Started	OK
2025-10-09 06:44:45	Fetching IPA icon path	OK
2025-10-09 06:44:45	Extracting String Metadata	OK
2025-10-09 06:44:45	Extracting URL and Email from IPA	OK
2025-10-09 06:44:45	Performing Malware check on extracted domains	OK
2025-10-09 06:44:57	Detecting Trackers from Domains	OK
2025-10-09 06:44:57	Saving to Database	OK

Report Generated by - MobSF v4.0.7

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.