MOBSF

IOS STATIC ANALYSIS REPORT

AI Cleaner (1.13.3)

File Name:	ai.cleaner.app_6448330325_1.13.3.ipa
Identifier:	ai.cleaner.app
Scan Date:	Jan. 11, 2025, 5:54 p.m.
App Security Score:	50/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	7	1	0	3

FILE INFORMATION

File Name: ai.cleaner.app_6448330325_1.13.3.ipa
Size: 129.27MB
MD5: b4ebecc60bfda1f85b6b260abcaa4774
SHA1: 954e0d17b209457cf428eb3e2cd8d32ea9dddcb5
SHA256: b458a967bb6e25a8444855f7658cfda3acfa56bdcc63911a05b522a39b6ea267

APP INFORMATION

App Name: AI Cleaner

App Type: Swift
Identifier: ai.cleaner.app
SDK Name: iphoneos18.2
Version: 1.13.3
Build: 1
Platform Version: 18.2
Min OS Version: 15.0
Supported Platforms: iPhoneOS,

BINARY INFORMATION

Arch: ARM64
Sub Arch: CPU_SUBTYPE_ARM64_ALL
Bit: 64-bit
Endian: <

#CUSTOM URL SCHEMES

URL NAME	SCHEMES
None Editor	aicleaner
None	fb899392691655683

APPLICATION PERMISSIONS

PERMISSIONS	STATUS	INFO	REASON IN MANIFEST
NSCalendarsUsageDescription	dangerous	Access Calendars.	This allows your completed calendar events to be found to free up storage.
NSCameraUsageDescription	dangerous	Access the Camera.	This allows the app to access the camera for AI object identification.
NSContactsUsageDescription	dangerous	Access Contacts.	This allows the app to analyse your contact details and identify duplicate or incomplete to optimise your contacts book.
NSPhotoLibraryUsageDescription	dangerous	Access the user's photo library.	This allows your excess photos and videos to be found to free up storage.

APP TRANSPORT SECURITY (ATS)

NO	ISSUE	SEVERITY	DESCRIPTION

IPA BINARY CODE ANALYSIS

HIGH: 0 | WARNING: 3 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	DESCRIPTION
1	Binary makes use of insecure API(s)	warning	**CWE:** CWE-676: Use of Potentially Dangerous Function **OWASP Top 10:** M7: Client Code Quality **OWASP MASVS:** MSTG-CODE-8	The binary may contain the following insecure API(s) _fopen , _memcpy , _printf , _sscanf , _stat , _strcpy , _strlen , _strncpy , _strtok , _vsnprintf , _wcslen
2	Binary makes use of the insecure Random function(s)	warning	**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) _srand
3	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.
4	Binary makes use of malloc function	warning	**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	False	info	The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.
PIE	True	info	The binary is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.
STACK CANARY	True	info	This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.
ARC	True	info	The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.
RPATH	True	warning	The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.
CODE SIGNATURE	True	info	This binary has a code signature.
ENCRYPTED	True	info	This binary is 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.

DYNAMIC LIBRARY & FRAMEWORK BINARY ANALYSIS

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
1	Payload/AI Cleaner.app/Frameworks/FBAEMKit.framework/FBAEMKit	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
2	Payload/AI Cleaner.app/Frameworks/OneSignalExtension.framework/OneSignalExtension	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
3	Payload/AI Cleaner.app/Frameworks/DMADecission.framework/DMADecission	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
4	Payload/AI Cleaner.app/Frameworks/OneSignalFramework.framework/OneSignalFramework	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
5	Payload/AI Cleaner.app/Frameworks/Lottie.framework/Lottie	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
6	Payload/AI Cleaner.app/Frameworks/grpc.framework/grpc	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	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.	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.	False info The binary does not have Runpath Search Path (@rpath) set.	True info This binary has a code signature.	False warning This binary is not encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
7	Payload/AI Cleaner.app/Frameworks/openssl_grpc.framework/openssl_grpc	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	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.	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.	False info The binary does not have Runpath Search Path (@rpath) set.	True info This binary has a code signature.	False warning This binary is not encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
8	Payload/AI Cleaner.app/Frameworks/OneSignalOSCore.framework/OneSignalOSCore	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
9	Payload/AI Cleaner.app/Frameworks/OneSignalNotifications.framework/OneSignalNotifications	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
10	Payload/AI Cleaner.app/Frameworks/FirebaseFirestoreInternal.framework/FirebaseFirestoreInternal	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	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.	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.	False info The binary does not have Runpath Search Path (@rpath) set.	True info This binary has a code signature.	False warning This binary is not encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
11	Payload/AI Cleaner.app/Frameworks/AppLovinSDK.framework/AppLovinSDK	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
12	Payload/AI Cleaner.app/Frameworks/AppLovinQualityService.framework/AppLovinQualityService	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
13	Payload/AI Cleaner.app/Frameworks/grpcpp.framework/grpcpp	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	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.	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.	False info The binary does not have Runpath Search Path (@rpath) set.	True info This binary has a code signature.	False warning This binary is not encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
14	Payload/AI Cleaner.app/Frameworks/FirebaseAnalytics.framework/FirebaseAnalytics	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	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.	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.	False info The binary does not have Runpath Search Path (@rpath) set.	True info This binary has a code signature.	False warning This binary is not encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
15	Payload/AI Cleaner.app/Frameworks/AdjustSigSdk.framework/AdjustSigSdk	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	False info The binary does not have Runpath Search Path (@rpath) set.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
16	Payload/AI Cleaner.app/Frameworks/OneSignalOutcomes.framework/OneSignalOutcomes	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
17	Payload/AI Cleaner.app/Frameworks/OneSignalInAppMessages.framework/OneSignalInAppMessages	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
18	Payload/AI Cleaner.app/Frameworks/FBSDKCoreKit.framework/FBSDKCoreKit	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
19	Payload/AI Cleaner.app/Frameworks/GoogleAppMeasurement.framework/GoogleAppMeasurement	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	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.	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.	False info The binary does not have Runpath Search Path (@rpath) set.	True info This binary has a code signature.	False warning This binary is not encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
20	Payload/AI Cleaner.app/Frameworks/OneSignalCore.framework/OneSignalCore	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
21	Payload/AI Cleaner.app/Frameworks/absl.framework/absl	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	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.	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.	False info The binary does not have Runpath Search Path (@rpath) set.	True info This binary has a code signature.	False warning This binary is not encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
22	Payload/AI Cleaner.app/Frameworks/RiveRuntime.framework/RiveRuntime	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
23	Payload/AI Cleaner.app/Frameworks/GoogleAppMeasurementIdentitySupport.framework/GoogleAppMeasurementIdentitySupport	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	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.	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.	False info The binary does not have Runpath Search Path (@rpath) set.	True info This binary has a code signature.	False warning This binary is not encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
24	Payload/AI Cleaner.app/Frameworks/OneSignalLiveActivities.framework/OneSignalLiveActivities	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
25	Payload/AI Cleaner.app/Frameworks/OneSignalUser.framework/OneSignalUser	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
26	Payload/AI Cleaner.app/Frameworks/FBSDKCoreKit_Basics.framework/FBSDKCoreKit_Basics	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	True info This binary is encrypted.	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
consent.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
img.shields.io	ok	**IP:** 104.21.80.27 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
consent.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
crl.comodoca.com	ok	**IP:** 104.18.38.233 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
consent.adjust.io	ok	**IP:** 185.151.204.1 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
adjust-skadnetwork.com	ok	**IP:** 185.151.204.50 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
consent.adjust.net.in	ok	**IP:** 185.151.204.30 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cocoapods.org	ok	**IP:** 104.26.1.240 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
crl.apple.com	ok	**IP:** 17.253.13.133 **Country:** United States of America **Region:** Florida **City:** Miami **Latitude:** 25.774269 **Longitude:** -80.193657 **View:** Google Map
ocsp.apple.com	ok	**IP:** 17.253.13.131 **Country:** United States of America **Region:** Florida **City:** Miami **Latitude:** 25.774269 **Longitude:** -80.193657 **View:** Google Map
crt.comodoca.com	ok	**IP:** 172.64.149.23 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
consent.adjust.com	ok	**IP:** 185.151.204.202 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
ocsp.comodoca.com0	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
consent.adjust.cn	ok	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
consent.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
www.apple.com	ok	**IP:** 23.37.124.29 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
consent.tr.adjust.com	ok	**IP:** 195.244.54.7 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
consent.adjust.world	ok	**IP:** 185.151.204.42 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
www.8	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
1@c.2iø	AI Cleaner.app/SF-Pro-Rounded-Thin.otf
+@l.kmn	AI Cleaner.app/SF-Pro-Rounded-Heavy.otf

EMAIL	FILE
moayad_kouz9@hotmail.com	AI Cleaner.app/README.md
moayad_kouz9@hotmail.com	AI Cleaner.app/LICENSE
g@wfgu.uϕi kp̈x@vp.6y v@zb.pw1hu q@xf.af szpm8@oel.7eq j@dy.îs oъ@d.dspddz 4dlq7-@ǧ.mt ɑ@rq.zyz5 2ⲭ@1q.3e vh@l.vjhwe h@9.ij f@q.tw5i 0@l.rr i@6j.qq c@9.m1t xzl@q.x9 jaoʒ@y.gi za@s.rb 1ⅎwzz@2.rjz7b□jῑo k@b.gi1w rлoř@ك.jф0□e 9@kg.pzz w@pc.nb gl@ke.yi s@g.lauf lcji@f.sml u@gw.rd ko@sc.ag a@jpbv.x5” usd@o.8q s7dx@oi20.fgrt p6@ky.pnr8 9xp4@ڸxw.rt pn@_n.w9 a@su0.9a kw@6.2e x@7b.ej k7@y.xfn 6r@yib.0ia ř@b0.ye95 qjb@v.qy qm@-.kkç o@mk.neqi ■@zsyh.rc44 z@bp.ytl □v8@e.jlj aj@k.cdh x@-.zh7 7@s.ħtf□3y p̈x@vo.ewr' i@c.ḷmó e@d.□ŋ l9eⲭ@w.vcl	

EMAIL	FILE
7c@rhm.uns hqs@qe.bvv t@9x.za ld@l.fz .7@w.ebm 8@qbmbçғy.0r ylao@k.xd ao_@hds1lii8.5n‘b 62h@kcl.r7 t5u@n.w_ g@gjn.n86h fک□ys@sd.zb 8o9@u.fh7 8l4ก@h.r1j hc@t.be q@cxhk.32s □@c.0hў̆co cui@s.8hp fkm@s.m4 u@z.af p@n3.nqe ru@8.jђg l@9.cr gcs@b.fmg 0o@t.ou t@ur.pmbklaʸ 5q@ë.zȯg ğ@05a.e2 mғbt3v3-a@tt.t4 z@e.qň fo+k@g.qj ɣntw@fi.bm ln6@vi._a 0_@hv.lru 0u@n.kk x□d@ɟ.wmp c@qo.2k0 h@q.zu xb@4a.nkh uvy@kjslƄysj.ce lx@ip.qt _qv@z9u.odbo s@1.wnl kxs@y.irl c@my.wĉbcgqq k@rr.hu ezd8@₸.iu u@p._wo _r@w25nun.nx w@a.bp y@_y-ny.g■gqkb t@z.wū□ +ъ@fma.im et1@v.ox b@ț8faiwb.ecl uk4v@_wrr.gt 0i@9qql.ns n@o□4■■б k□@h2.pngm jh@x2.s1 h@j3.zerka	AI Cleaner.app/AI Cleaner

EMAIL	FILE
gq@zj.xôə +cɪgf@qygk.vl x@-.vdmk 0t@h0.hgd d@u.git9wd zq@d.rl3m□ j@y.w4 8@zul.nнjý b+t@p.lpi x@l.ky i9_@k.x5l y@qm4z.wr gκ7@lrr7.ue g3d@l.iyr i@bi4.ti 4yn☃@i.qs eb@x1.vk x6@bh.zgg 0@w.np dui@u.to¼f -@g.g‖4 u@l0b.ru ɯeq@3.2fx m@nd7.nɇw c@ᵽ.a8p wo@i.x5ej 4f@k.0h e@66m.g2 ïphw@2eb.ɠ6a xóuy@pi.p9bz j@ڰsbbr7.rī f@l.wi z@f□.xнk 0@k.lc1sm 55@k.5h p@ndnp.tndhf7 8@o.2e b2@jj5.qj p@whj.dum +so@sz□hil.vs u@f.sj3 n@dh.45lf .@q.avc e@btnw.jv0 л23@32.eem 7@t.hq j341sȧedu.w@w7v.g8 io@s.pr rvu6lvp@jg.ox8 ƥx@gu0kj.fj qj@cpl.nv hw@-.ryώ ر@w.z2b o@yup.n5□c_ ej@y0.1ujjl ccts@im7gq.r0s z@d.mv cly■@q.bq y@n.xqff j@uo.2g 2pob@6.ctwho	

EMAIL	FILE
ŋ@f.gh8 pkg@u.rf94.y0ч0e vg@tbb.iydq v@5.5d aɛƒbbⱬkpo@w.rvq m@wœm.ixana f@cb.n4 f@0.rnюdhv k@t.lkw9l5o lrsn-aĭz@e.ժi i@mq_.ed o@w.xe9 6q@x.qλ 5@ě.kɀ 5@l.h8 e@b.wz7z il@l._aaf 3f@gxl.1sʒm4 f@0v.fj bg@na.ԋgg x@n.vs6n l8s@09.0l hfo@n.woxd cmogym@lvl.taaq4 dz@9.hɛ b1@6.zl فr@1.rs_w y3ת1hwpvelc4@z.4uit3 6jk_@3rm.3sb xs@cü.pt ˇo@.ců p@6z.mhxx m8@ös.sɱl n@ir._zqe5 +@7k.sh c@yuq.mf r@qqr.ej dy@.ut ztpb+j@gn.obbs r@e.omkirj ottb@sbl.jgac f@0ty.sbǽ fy@0.6ƾz b@s.nwpx c8d@kwes.gd	
e+t@ue.дb k@m.xb a@k0.tʾ	AI Cleaner.app/SC_Info/AI Cleaner.supf
k@m.xb a@k0.tʾ	AI Cleaner.app/SC_Info/AI Cleaner.supp
l@9.cr y@n.xq f@q.tw5i 8@o.2e h@j3.zer x@-.vd vh@l.vj 4@z.4u	IPA Strings Dump

EMAIL	FILE
4p@a.g0	Payload/AI Cleaner.app/Frameworks/FBSDKCoreKit.framework/FBSDKCoreKit

TRACKERS

TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52

HARDCODED SECRETS

POSSIBLE SECRETS
amplitudeApiKey : vnvVzUk++DqlbCeSh1WjqByy0g9TtJSF3RkLwAh7wMzK/seNcHbWwqDAw95OSI5J
ads_show_interstitial_secret_space : 0
AdjustAppToken : 0KVZN4eCG/QSxpsu0cGxpg==
API_KEY : AIzaSyDYx1wAllDNYcL2UDwMH33wAOvnr-ZhsFE
FacebookClientToken : 6ccbe81fa0b500c5f71b04f1d3ec1d97
revenuekitApiKey : cTfSWol+joSxBx75phd/8Dz1cldC+RPeDl95hwGHaRPC3BsjS9dt7PEfOn7dldlJ
secret_gallery_daily_limit : 2
ads_rewarded_secret_gallery_quota : 0

APP STORE INFORMATION

Title: AI Cleaner: Clean Up Storage

Score: 4.59701 **Features:** **Price:** 0.0 **Category:** Utilities, Productivity,
App Store URL: ai.cleaner.app

Developer: GRIMLAX TRADE, S.L.
Developer ID: 1684438177
Developer Website: https://aicleaner.app/
Developer URL: https://apps.apple.com/us/developer/grimlax-trade-s-l/id1684438177?uo=4
Supported Devices iPhone5s-iPhone5s, iPadAir-iPadAir, iPadAirCellular-iPadAirCellular, iPadMiniRetina-iPadMiniRetina, iPadMiniRetinaCellular-iPadMiniRetinaCellular, iPhone6-iPhone6, iPhone6Plus-iPhone6Plus, iPadAir2-iPadAir2, iPadAir2Cellular-iPadAir2Cellular, iPadMini3-iPadMini3, iPadMini3Cellular-iPadMini3Cellular, iPodTouchSixthGen-iPodTouchSixthGen, iPhone6s-iPhone6s, iPhone6sPlus-iPhone6sPlus, iPadMini4-iPadMini4, iPadMini4Cellular-iPadMini4Cellular, iPadPro-iPadPro, iPadProCellular-iPadProCellular, iPadPro97-iPadPro97, iPadPro97Cellular-iPadPro97Cellular, iPhoneSE-iPhoneSE, iPhone7-iPhone7, iPhone7Plus-iPhone7Plus, iPad611-iPad611, iPad612-iPad612, iPad71-iPad71, iPad72-iPad72, iPad73-iPad73, iPad74-iPad74, iPhone8-iPhone8, iPhone8Plus-iPhone8Plus, iPhoneX-iPhoneX, iPad75-iPad75, iPad76-iPad76, iPhoneXS-iPhoneXS, iPhoneXSMax-iPhoneXSMax, iPhoneXR-iPhoneXR, iPad812-iPad812, iPad834-iPad834, iPad856-iPad856, iPad878-iPad878, iPadMini5-iPadMini5, iPadMini5Cellular-iPadMini5Cellular, iPadAir3-iPadAir3, iPadAir3Cellular-iPadAir3Cellular, iPodTouchSeventhGen-iPodTouchSeventhGen, iPhone11-iPhone11, iPhone11Pro-iPhone11Pro, iPadSeventhGen-iPadSeventhGen, iPadSeventhGenCellular-iPadSeventhGenCellular,

iPhone11ProMax-iPhone11ProMax, iPhoneSESecondGen-iPhoneSESecondGen, iPadProSecondGen-iPadProSecondGen, iPadProSecondGenCellular-iPadProSecondGenCellular, iPadProFourthGen-iPadProFourthGen, iPadProFourthGenCellular-iPadProFourthGenCellular, iPhone12Mini-iPhone12Mini, iPhone12-iPhone12, iPhone12Pro-iPhone12Pro, iPhone12ProMax-iPhone12ProMax, iPadAir4-iPadAir4, iPadAir4Cellular-iPadAir4Cellular, iPadEighthGen-iPadEighthGen, iPadEighthGenCellular-iPadEighthGenCellular, iPadProThirdGen-iPadProThirdGen, iPadProThirdGenCellular-iPadProThirdGenCellular, iPadProFifthGen-iPadProFifthGen, iPadProFifthGenCellular-iPadProFifthGenCellular, iPhone13Pro-iPhone13Pro, iPhone13ProMax-iPhone13ProMax, iPhone13Mini-iPhone13Mini, iPhone13-iPhone13, iPadMiniSixthGen-iPadMiniSixthGen, iPadMiniSixthGenCellular-iPadMiniSixthGenCellular, iPadNinthGen-iPadNinthGen, iPadNinthGenCellular-iPadNinthGenCellular, iPhoneSEThirdGen-iPhoneSEThirdGen, iPadAirFifthGen-iPadAirFifthGen, iPadAirFifthGenCellular-iPadAirFifthGenCellular, iPhone14-iPhone14, iPhone14Plus-iPhone14Plus, iPhone14Pro-iPhone14Pro, iPhone14ProMax-iPhone14ProMax, iPadTenthGen-iPadTenthGen, iPadTenthGenCellular-iPadTenthGenCellular, iPadPro11FourthGen-iPadPro11FourthGen, iPadPro11FourthGenCellular-iPadPro11FourthGenCellular, iPadProSixthGen-iPadProSixthGen, iPadProSixthGenCellular-iPadProSixthGenCellular, iPhone15-iPhone15, iPhone15Plus-iPhone15Plus, iPhone15Pro-iPhone15Pro, iPhone15ProMax-iPhone15ProMax, iPadAir11M2-iPadAir11M2, iPadAir11M2Cellular-iPadAir11M2Cellular, iPadAir13M2-iPadAir13M2, iPadAir13M2Cellular-iPadAir13M2Cellular, iPadPro11M4-iPadPro11M4, iPadPro11M4Cellular-iPadPro11M4Cellular, iPadPro13M4-iPadPro13M4, iPadPro13M4Cellular-iPadPro13M4Cellular, iPhone16-iPhone16, iPhone16Plus-iPhone16Plus, iPhone16Pro-iPhone16Pro, iPhone16ProMax-iPhone16ProMax, iPadMiniA17Pro-iPadMiniA17Pro, iPadMiniA17ProCellular-iPadMiniA17ProCellular,

Description:

Do you often find your iPhone running out of storage? AI Cleaner offers AI-powered cleaning unlike any other. With powerful cleaning functions, it helps you optimize your phone's performance by removing unnecessary files. → Reclaim space and enjoy a faster, more efficient device with optimized performance. ■ KEY FEATURES » AI Smart Cleaner » Remove Duplicate Photos & Videos » Contact Cleanup » Event Remover » Protect files with secret storage » Compress Photos & Videos SMART CLEANING Experience the power of AI with AI Cleaner, designed to deliver the quickest and most effective cleanup for your iPhone. If you want a thorough clean, our comprehensive cleaning feature uses all the app functions simultaneously, ensuring maximum storage recovery in minimal time. DELETE DUPLICATE PHOTOS AND VIDEOS AI Cleaner app scans your gallery for duplicate photos and videos, allowing you to delete them with a single tap. Free up space without losing your memories. CONTACT MANAGEMENT Forget about incomplete and duplicate contacts cluttering your address book. AI Cleaner identifies and helps you clean up your contact list to keep it organized and relevant. REMOVE PAST EVENTS Is your calendar crowded with obsolete past events? AI Cleaner quickly detects and removes old events, freeing up space on your schedule. PROTECT PHOTOS, VIDEOS AND CONTACTS Effortlessly safeguard your memories and sensitive information by protecting and concealing your photos, videos, and contacts within a private storage space, ensuring an extra layer of security and privacy. Relax, knowing your memories are secured from unwanted access. COMPRESS PHOTOS AND VIDEOS Regain precious memory on your phone with just a few clicks by compressing your photos and videos! Select from a variety of compression levels—high, medium, or low—to suit your storage preferences and free up space seamlessly. ■ EFFORTLESS STORAGE MANAGEMENT » Easy to use: With our intuitive interface, you can easily free up space manually or with AI assistance. » AI-Powered cleaning: AI Cleaner efficiently scans your device to identify duplicate and unwanted items. » Data security: Your personal data is safe with us. AI Cleaner does not store your personal information. » Performance optimization: Improve your iPhone's speed and responsiveness with AI Cleaner app. Our advanced AI technology, frees up gigabytes of storage in seconds. » Regular updates: We keep AI Cleaner up to date with the latest improvements and features to ensure the best experience. ■ CONTACT: For app support and more information, reach out to us at: info@aicleaner.app Terms of Use: https://aicleaner.app/terms-of-use Privacy Policy: https://aicleaner.app/privacy-policy Download AI Cleaner now and enjoy a faster and more efficient device! Free up space, organize your gallery and agenda, and keep your mobile at its best.

SCAN LOGS

Timestamp	Event	Error
2025-01-11 17:54:30	iOS Binary (IPA) Analysis Started	OK
2025-01-11 17:54:30	Generating Hashes	OK
2025-01-11 17:54:30	Extracting IPA	OK
2025-01-11 17:54:30	Unzipping	OK
2025-01-11 17:54:31	iOS File Analysis and Normalization	OK
2025-01-11 17:54:31	iOS Info.plist Analysis Started	OK
2025-01-11 17:54:31	Finding Info.plist in iOS Binary	OK
2025-01-11 17:54:31	Fetching Details from App Store: ai.cleaner.app	OK

2025-01-11 17:54:31	Searching for secrets in plist files	OK
2025-01-11 17:54:31	Starting Binary Analysis	OK
2025-01-11 17:54:34	Dumping Classes from the binary	OK
2025-01-11 17:54:34	Running jtool against the binary for dumping classes	OK
2025-01-11 17:54:38	Library Binary Analysis Started	OK
2025-01-11 17:54:38	Framework Binary Analysis Started	OK
2025-01-11 17:54:38	Analyzing Payload/AI Cleaner.app/Frameworks/FBAEMKit.framework/FBAEMKit	OK
2025-01-11 17:54:38	Analyzing Payload/AI Cleaner.app/Frameworks/OneSignalExtension.framework/OneSignalExtension	OK
2025-01-11 17:54:38	Analyzing Payload/AI Cleaner.app/Frameworks/DMADecission.framework/DMADecission	OK
2025-01-11 17:54:38	Analyzing Payload/AI Cleaner.app/Frameworks/OneSignalFramework.framework/OneSignalFramework	OK
2025-01-11 17:54:38	Analyzing Payload/AI Cleaner.app/Frameworks/Lottie.framework/Lottie	OK
2025-01-11 17:54:38	Analyzing Payload/AI Cleaner.app/Frameworks/grpc.framework/grpc	OK
2025-01-11 17:54:38	Analyzing Payload/AI Cleaner.app/Frameworks/openssl_grpc.framework/openssl_grpc	OK
2025-01-11 17:54:38	Analyzing Payload/AI Cleaner.app/Frameworks/OneSignalOSCore.framework/OneSignalOSCore	OK
2025-01-11 17:54:38	Analyzing Payload/AI Cleaner.app/Frameworks/OneSignalNotifications.framework/OneSignalNotifications	OK
2025-01-11 17:54:38	Analyzing Payload/AI Cleaner.app/Frameworks/FirebaseFirestoreInternal.framework/FirebaseFirestoreInternal	OK

2025-01-11 17:54:38	Analyzing Payload/AI Cleaner.app/Frameworks/AppLovinSDK.framework/AppLovinSDK	OK
2025-01-11 17:54:38	Analyzing Payload/AI Cleaner.app/Frameworks/AppLovinQualityService.framework/AppLovinQualityService	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/grpcpp.framework/grpcpp	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/FirebaseAnalytics.framework/FirebaseAnalytics	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/AdjustSigSdk.framework/AdjustSigSdk	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/OneSignalOutcomes.framework/OneSignalOutcomes	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/OneSignalInAppMessages.framework/OneSignalInAppMessages	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/FBSDKCoreKit.framework/FBSDKCoreKit	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/GoogleAppMeasurement.framework/GoogleAppMeasurement	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/OneSignalCore.framework/OneSignalCore	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/absl.framework/absl	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/RiveRuntime.framework/RiveRuntime	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/GoogleAppMeasurementIdentitySupport.framework/GoogleAppMeasurementIdentitySupport	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/OneSignalLiveActivities.framework/OneSignalLiveActivities	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/OneSignalUser.framework/OneSignalUser	OK
2025-01-11 17:54:39	Analyzing Payload/AI Cleaner.app/Frameworks/FBSDKCoreKit_Basics.framework/FBSDKCoreKit_Basics	OK
2025-01-11 17:54:39	Extracting String Metadata	OK

2025-01-11 17:54:39	Extracting URL and Email from IPA	OK
2025-01-11 17:54:56	Performing Malware check on extracted domains	OK
2025-01-11 17:55:03	Fetching IPA icon path	OK
2025-01-11 17:55:04	Detecting Trackers from Domains	OK
2025-01-11 17:55:04	Saving to Database	OK