IOS STATIC ANALYSIS REPORT

AI Cleaner (3.2.1)

File Name:	aicleanupphonestorage_6496865463_3.2.1.ipa
Identifier:	aicleanupphonestorage
Scan Date:	Jan. 11, 2025, 5:53 p.m.
App Security Score:	**52/100 (MEDIUM RISK)**

Grade: **B**

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	6	1	1	1

FILE INFORMATION

File Name: aicleanupphonestorage_6496865463_3.2.1.ipa
Size: 96.45MB
MD5: a61bc2576d5ad66376659835f2d34385
SHA1: bd6a657f0fdfd7e763746e83e61438aaeab770cb
SHA256: ceee52a702fceeb5903dd4707e6543e97a6332e6cd599b63d2eeb7394c1906e8

APP INFORMATION

App Name: AI Cleaner
App Type: Swift
Identifier: aicleanupphonestorage
SDK Name: iphoneos17.4

Version: 3.2.1
Build: 321157
Platform Version: 17.4
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	com.googleusercontent.apps.539520795862-bkfvhi0g2utkj3r15icmvnmumchi59q9 fb448046254445642

APPLICATION PERMISSIONS

PERMISSIONS	STATUS	INFO	REASON IN MANIFEST
NSCalendarsUsageDescription	dangerous	Access Calendars.	We need access to your calendar to manage and view your schedule
NSCameraUsageDescription	dangerous	Access the Camera.	AI Cleaner needs access to your camera so you can start taking photos and videos to save them in your Privacy Space
NSContactsUsageDescription	dangerous	Access Contacts.	Get contact permission to modify contact information
NSFaceIDUsageDescription	normal	Access the ability to authenticate with Face ID.	face id
NSMicrophoneUsageDescription	dangerous	Access microphone.	Get Microphone permission for record video
NSPhotoLibraryUsageDescription	dangerous	Access the user's photo library.	Get album permission for photo collation and compression

APP TRANSPORT SECURITY (ATS)

HIGH: **1** | WARNING: **0** | INFO: **0** | SECURE: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App Transport Security AllowsArbitraryLoads is allowed	high	App Transport Security restrictions are disabled for all network connections. Disabling ATS means that unsecured HTTP connections are allowed. HTTPS connections are also allowed, and are still subject to default server trust evaluation. However, extended security checks like requiring a minimum Transport Layer Security (TLS) protocol version—are disabled. This setting is not applicable to domains listed in NSExceptionDomains.

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 , _sprintf , _sscanf , _stat , _strcpy , _strlen , _strncpy , _vsnprintf
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) _random , _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	SYM STRI
1	Payload/cleanPhone.app/Frameworks/GCDWebServer.framework/GCDWebServer	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 warnin Debug Symbo availal strip debug symbo Strip D Symbo During YES, Deplo Postpr to YES Strip L Produ in pro build s

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
2	Payload/cleanPhone.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 warnin Debug Symbo availal strip debug symbo Strip D Symbo During YES, Deplo Postpr to YES Strip L Produ in pro build s

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
3	Payload/cleanPhone.app/Frameworks/libavutil.framework/libavutil	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.	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.	True info This binary is encrypted.	False warni Debug Symbo availa strip debug symbo Strip D Symbo During YES, Deplo Postpr to YES Strip L Produ in pro build

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
4	Payload/cleanPhone.app/Frameworks/ffmpegkit.framework/ffmpegkit	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 warnir Debug Symbo availal strip debug symbo Strip D Symbo During YES, Deplo Postpr to YES Strip L Produ in pro build s

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
5	Payload/cleanPhone.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 warnin Debug Symb availa strip debug symb Strip D Symb Durin YES, Deplo Postp to YES Strip L Produ in pro build

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
6	Payload/cleanPhone.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 warni Debug Symbo availa strip debug symbo Strip D Symbo During YES, Deplo Postpr to YES Strip L Produ in pro build

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
7	Payload/cleanPhone.app/Frameworks/GoogleAppMeasurementOnDeviceConversion.framework/GoogleAppMeasurementOnDeviceConversion	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 warni Debug Symbo availa strip debug symbo Strip D Symbo During YES, Deplo Postpr to YES Strip L Produ in pro build

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
8	Payload/cleanPhone.app/Frameworks/libswresample.framework/libswresample	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.	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.	True info This binary is encrypted.	False warni Debug Symbo availa strip debug symbo Strip D Symbo During YES, Deplo Postpr to YES Strip L Produ in pro build

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
9	Payload/cleanPhone.app/Frameworks/libavcodec.framework/libavcodec	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.	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.	True info This binary is encrypted.	False warni Debu Symb availa strip debu symb Strip Symb Durin YES, Deplo Postp to YES Strip Produ in pro build

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
10	Payload/cleanPhone.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 warni Debu Symb availa strip debug symb Strip Symb Durin YES, Deplo Postp to YES Strip Produ in pro build

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
11	Payload/cleanPhone.app/Frameworks/libavdevice.framework/libavdevice	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 warni Debug Symbo availa strip debug symbo Strip D Symbo During YES, Deplo Postpr to YES Strip L Produ in pro build

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
12	Payload/cleanPhone.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 warni Debug Symb availa strip debug symb Strip D Symb Durin YES, Deplo Postp to YES Strip L Produ in pro build

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
13	Payload/cleanPhone.app/Frameworks/libswscale.framework/libswscale	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.	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.	True info This binary is encrypted.	False warnin Debug Symbo availa strip debug symbo Strip D Symbo During YES, Deplo Postpr to YES Strip L Produ in pro build s

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
14	Payload/cleanPhone.app/Frameworks/libavformat.framework/libavformat	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.	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.	True info This binary is encrypted.	False warni Debug Symbo availa strip debug symbo Strip D Symbo During YES, Deplo Postpr to YES Strip L Produ in proj build s

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
15	Payload/cleanPhone.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 warnir Debug Symb availal strip debug symbo Strip D Symbo During YES, Deplo Postpr to YES Strip L Produ in proj build s

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
16	Payload/cleanPhone.app/Frameworks/FMDB.framework/FMDB	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 warnin Debug Symbo availa strip debug symbo Strip D Symbo During YES, Deplo Postpr to YES Strip L Produ in pro build

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
17	Payload/cleanPhone.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 warnir Debug Symbo availal strip debug symbo Strip D Symbo During YES, Deplo Postpr to YES Strip L Produ in pro build s

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYM STRI
18	Payload/cleanPhone.app/Frameworks/libavfilter.framework/libavfilter	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.	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.	True info This binary is encrypted.	False warnin Debug Symbo availab strip debug symbo Strip D Symbo During YES, Deploy Postpr to YES Strip L Produ in proj build s

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
api-sdk.aicleanup.net	ok	**IP:** 47.252.113.195 **Country:** United States of America **Region:** California **City:** San Mateo **Latitude:** 37.547424 **Longitude:** -122.330589 **View:** Google Map
crl.apple.com	ok	**IP:** 17.253.13.139 **Country:** United States of America **Region:** Florida **City:** Miami **Latitude:** 25.774269 **Longitude:** -80.193657 **View:** Google Map
postbacks-app.com	ok	**IP:** 34.117.147.68 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
ocsp.apple.com	ok	**IP:** 17.253.13.142 **Country:** United States of America **Region:** Florida **City:** Miami **Latitude:** 25.774269 **Longitude:** -80.193657 **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

✉ EMAILS

EMAIL	FILE
ldb@8.w4 m@p.upi a@6.aac e@j.op h@e.h4 v@b.s5hi■ lsm6tkm@q.7y ayw@a.dw n@g6.wye 0cw@ij5g.be	

EMAIL	FILE
ba@i.5gʒk	
eiiq@n.4i	
8@g.iqi	
xҗe@7.[redacted] z8z	
o@nec.tmzüj	
f@j.q5g	
6@70.dg39	
6@6utx.f1j	
x3@s.mk	
qc@sn.wz	
t.@u.5mf	
m@ámh.ps	
zp@gl.bnuk	
h@l.ztĸ	
dɩɛa1s@r.z_nujcp	
wp@ɒ.sb	
u@eoʗ.zgt	
4@c.2ơ	
+0aӈ@i.tpt	
yssj@2.h7	
oqo@5f9f.a5	
gʔa@sʉ.p0	
n@lr.am	
gch@96b.tn	
8tt[redacted] @s27y.hg	
ly@ûcqx.mu	
wo@za.fh	
n@3.hb	
m@nm.ӊ0d	
jmro@c.ffkf	
x@e.tq03	
u[redacted] l@-.ao	
ynj2d@ƙy.3∇h	
pxy@3.0t	
h@k.tca	
ur@ew.ns	
q@q.cjdf	
3@r.Ɩlezz	
fdg@ap.ht	
t@q.79j	
r@ɋgn9.xx	
+n@9y.ÿ4	
ȕ@j.6hu	
eh_l4@vdw.bӽ	
3@apzxw.ng	
4zv@s.tbȍx	
-mg@s.80	
w@a.yutꞔ	
p@u.niv	
q@f.aṻ	
ꝑ@4.lwqsl	
k0@h.vv	
5@9.җ4	
z@e.uz	
7ajv@ʋ._m	
hf@ï.qxy36yq	
8@p.dɺ	
-i@57_m.o80	
w@z.0ч	
z@m8.xv	
p0@wk.wt	
st8@3kuqė.ыg	
o@я.bnt	
+xl@k.wh	
tg-@wue.1mc2ppc	
--@1d.āo3hȡ	

EMAIL	FILE
q@azdb_is.ʊl 5@jmγ.0fφu dž@v8.ux q@h.ca s7@cm.dh -r@v.xs r7@e.23k5sjpper ns@e.xaq ma9@eeu3.tw dkap@o.1u 3@u.1h aɾxh@wu.idoy 6@y.e0 a@y1k7.gvs l@s.oxs qǎƈ@to.m0g w8@پn.xc pf@nl.ems9 gca@t0.tu b@u0.kr2ڵ k@6ϐ.wu w@ɹwx.ȧe u@qm.ieo! xt1@9aﻫeu.dfw dyq@pr.e2 g_@k._h yf@o.oyd kcf@r.xi x@k.uju f@8au.bn wu@5mz.x he@b.wx _z@g.fj f@o.ba x-x@xz.fyɓځfq yks@p.zm n@gq2q.ha fs@ч.9c t@s.ee f@b.iv0 c7@7.u4 g@v.okcz3h j@v3x.qoq n_@l.caa čiu@qc.sn k@5.nt so@ik.ob ey@br.ꞷ6 r@et.kt8 ¾rr@i.pn n@p.na8 oyg@ң.5w g@m.yqi r@us.lx v@zsd.xb ƽ@qx.rs c@i.g5rъ _n1@m.ne g@g.рю 3@wl.javr püű@nac6.l7gԳzj ze@t-.٣ή 33@im.zxeak g@wdgi.nsʷ +@й.ol	cleanPhone.app/cleanPhone

EMAIL	FILE
7@cr.86 0@a.zr▯n z■■■@86we.sqs qv@yɛ.g4ɱsct_▯ trx@smhfi_.cű sz@s.3me us0@ia.ny lvd@v.q▯e z@ꞔ.s6af m-o@w.ol bk@nc.ɥo y˛t+@v.u14 _@b0.y4 vpwj@i.1ic uwbk@-c.t▯gw dx@▯bg.dlamjb1 v@oh.s4m 3z@f.sd +@fqi.61r lcp@g.6q ɟjp@j.ĸbm 4@y6r.4mv j-@l.wњ vut@g.ldft s@d.cdf▯ y@hf.gi s@4d.amqw d@6.nr _@nib.wct h@be.fwbj6 nss6gb@ĸ.bnooa9hg4n vj.tȉ@5.fv▯vczsd0o sp@wm.5t iʘ@k.n■ 3@lӂ.▯p ▯cw@■.xl t@ν.vk l3u@ƿn6._9 g@ɔqxuy.kp g■w86@k.bj xx@hs.t3 qg@gvq.kzcxn d@-.tgm js@lx.lx mq@cfkgd.vva8 6@v.v▯ hy@vms.2p rdb.rgfy@ӂ.ƌ½	
1@2x_1.png	cleanPhone.app/page_pro_btn.json
72@3x.png 47750@3x.png	cleanPhone.app/safe_check.json
l@s.oxs g@m.yqi	IPA Strings Dump

HARDCODED SECRETS

POSSIBLE SECRETS
APPFYLYER_KEY_ID : WwPpkxWPk8mj3dU5QxjKXg
AppKey : hHECxgxYVYGjUDcNDRGLLsengNtKjXcG
API_KEY : AIzaSyC_dle_1ByZEzaZK5imguhB5eoGyKF1u6M
FacebookClientToken : 94c82dc68a2131d041705091940f1306
FacebookClientToken : CLIENT-TOKEN

APP STORE INFORMATION

Title: AI Cleaner: Storage Cleaner

Score: 4.28589 **Features:** **Price:** 0.0 **Category:** Utilities, Productivity,
App Store URL: aicleanupphonestorage

Developer: □ □
Developer ID: 1725351707
Developer Website: https://dfd206ef0.app-ads-txt.com
Developer URL: https://apps.apple.com/us/developer/%E5%A8%9C-%E7%9F%B3/id1725351707?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:

AI Cleaner is your ideal choice for managing photos on your iOS device, offering a comprehensive solution to photo clutter. Over time, our albums can become cluttered with numerous similar or duplicate photos and screenshots, consuming valuable storage space and making photo organization difficult. The arrival of AI Cleaner will change this situation entirely. ■ KEY FEATURES Similar Photo Cleanup: AI Cleaner can quickly and accurately identify and remove similar photos. Whether they're consecutive shots or slightly different images, AI Cleaner can pinpoint and eliminate redundant content, freeing up valuable storage space. Duplicate Photo Cleanup: Accidentally saved multiple identical photos? No worries! AI Cleaner detects and removes duplicate photos to keep your photo library neat and organized. Similar Screenshot Cleanup: Similar screenshots can also clutter your album and consume storage space. AI Cleaner helps you effortlessly identify and clean up similar screenshots, keeping your album tidy. Similar and Other Video Cleanup: AI Cleaner identifies and cleans similar or space-consuming video files, helping you efficiently manage your phone's storage. Video Compression: Reduce large video file sizes without losing quality. AI Cleaner offers easy-to-use compression tools to help free up space while keeping your favorite videos on your device. Private Space: Securely store sensitive photos and videos in AI Cleaner's Privacy Space. ***Data Security: Your photos won't be uploaded to our servers, ensuring your privacy.*** ***You may cancel your subscription at any time*** All payments made through the app are controlled and managed by Apple Subscription automatically renews unless auto-renew is turned off at least 24 hours before the end of the current period Account will be charged for renewal 24 hours prior to the end of the current period You can manage your subscriptions by App Store > Apple Id > Subscriptions Privacy Agreement: https://privacy.aicleanup.net User Agreement: https://sites.google.com/view/terms4aicleaner Automatic renewal agreement: https://sites.google.com/view/sub-agreement-aicleaner

SCAN LOGS

Timestamp	Event	Error
2025-01-11 17:53:16	iOS Binary (IPA) Analysis Started	OK

2025-01-11 17:53:16	Generating Hashes	OK
2025-01-11 17:53:16	Extracting IPA	OK
2025-01-11 17:53:16	Unzipping	OK
2025-01-11 17:53:17	iOS File Analysis and Normalization	OK
2025-01-11 17:53:17	iOS Info.plist Analysis Started	OK
2025-01-11 17:53:17	Finding Info.plist in iOS Binary	OK
2025-01-11 17:53:17	Fetching Details from App Store: aicleanupphonestorage	OK
2025-01-11 17:53:17	Searching for secrets in plist files	OK
2025-01-11 17:53:17	Starting Binary Analysis	OK
2025-01-11 17:53:17	Dumping Classes from the binary	OK
2025-01-11 17:53:17	Running jtool against the binary for dumping classes	OK
2025-01-11 17:53:21	Library Binary Analysis Started	OK
2025-01-11 17:53:21	Framework Binary Analysis Started	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/GCDWebServer.framework/GCDWebServer	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/FBAEMKit.framework/FBAEMKit	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/libavutil.framework/libavutil	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/ffmpegkit.framework/ffmpegkit	OK

2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/AppLovinSDK.framework/AppLovinSDK	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/FirebaseAnalytics.framework/FirebaseAnalytics	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/GoogleAppMeasurementOnDeviceConversion.framework/GoogleAppMeasurementOnDeviceConversion	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/libswresample.framework/libswresample	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/libavcodec.framework/libavcodec	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/FBSDKCoreKit.framework/FBSDKCoreKit	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/libavdevice.framework/libavdevice	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/GoogleAppMeasurement.framework/GoogleAppMeasurement	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/libswscale.framework/libswscale	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/libavformat.framework/libavformat	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/GoogleAppMeasurementIdentitySupport.framework/GoogleAppMeasurementIdentitySupport	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/FMDB.framework/FMDB	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/FBSDKCoreKit_Basics.framework/FBSDKCoreKit_Basics	OK
2025-01-11 17:53:21	Analyzing Payload/cleanPhone.app/Frameworks/libavfilter.framework/libavfilter	OK
2025-01-11 17:53:21	Extracting String Metadata	OK
2025-01-11 17:53:21	Extracting URL and Email from IPA	OK
2025-01-11 17:53:25	Performing Malware check on extracted domains	OK

2025-01-11 17:53:28	Fetching IPA icon path	OK
2025-01-11 17:53:29	Detecting Trackers from Domains	OK
2025-01-11 17:53:29	Saving to Database	OK

Report Generated by - MobSF v4.2.9

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.