MOBSF

IOS STATIC ANALYSIS REPORT

Cleaner Guru (2.6.0)

File Name:	gen.universe.app.cleaner_1476380919_2.6.0.ipa
Identifier:	gen.universe.app.cleaner
Scan Date:	Jan. 11, 2025, 11:30 a.m.

App Security Score: 64/100 (LOW RISK)

Grade: A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	4	2	1	2

FILE INFORMATION

File Name: gen.universe.app.cleaner_1476380919_2.6.0.ipa
Size: 166.56MB
MD5: 73bcf03a26872b7377fa57329a1db510
SHA1: 2adebbc912d5f9d14b8448a8ff239290aa60d1bd

SHA256: 1dc6957a6f50b331306e9f5d00edfd2e1961df0a9bdd8708e69b74597baf6966

APP INFORMATION

App Name: Cleaner Guru
App Type: Swift
Identifier: gen.universe.app.cleaner
SDK Name: iphoneos18.0
Version: 2.6.0
Build: 237
Platform Version: 18.0
Min OS Version: 16.0
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.1035494693391-cfm5aid528mcqsiac5ri91qnubfru8ov

APPLICATION PERMISSIONS

PERMISSIONS	STATUS	INFO	REASON IN MANIFEST
NSContactsUsageDescription	dangerous	Access Contacts.	In order to find duplicate and empty contacts the app need an access to Contacts
NSPhotoLibraryUsageDescription	dangerous	Access the user's photo library.	In order to find duplicate the app needs an access to Gallery

APP TRANSPORT SECURITY (ATS)

NO	ISSUE	SEVERITY	DESCRIPTION

</> IPA BINARY CODE ANALYSIS

HIGH: **0** | WARNING: **2** | 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 , _strlen , _strncpy
2	Binary makes use of Logging function	info	**CWE:** CWE-532: Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3	The binary may use _NSLog function for logging.
3	Binary makes use of malloc function	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.

PROTECTION	STATUS	SEVERITY	DESCRIPTION
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/Cleaner Guru.app/Frameworks/NVActivityIndicatorView.framework/NVActivityIndicatorView	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/Cleaner Guru.app/Frameworks/GoogleDataTransport.framework/GoogleDataTransport	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/Cleaner Guru.app/Frameworks/PrettyCards.framework/PrettyCards	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/Cleaner Guru.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
5	Payload/Cleaner Guru.app/Frameworks/FirebaseSessions.framework/FirebaseSessions	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/Cleaner Guru.app/Frameworks/AdvancedPageControl.framework/AdvancedPageControl	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
7	Payload/Cleaner Guru.app/Frameworks/JTAppleCalendar.framework/JTAppleCalendar	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
8	Payload/Cleaner Guru.app/Frameworks/nanopb.framework/nanopb	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.	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/Cleaner Guru.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
10	Payload/Cleaner Guru.app/Frameworks/Promises.framework/Promises	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
11	Payload/Cleaner Guru.app/Frameworks/FirebaseABTesting.framework/FirebaseABTesting	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/Cleaner Guru.app/Frameworks/FirebaseSharedSwift.framework/FirebaseSharedSwift	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/Cleaner Guru.app/Frameworks/SwiftMessages.framework/SwiftMessages	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
14	Payload/Cleaner Guru.app/Frameworks/FirebaseCoreInternal.framework/FirebaseCoreInternal	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
15	Payload/Cleaner Guru.app/Frameworks/FirebaseRemoteConfig.framework/FirebaseRemoteConfig	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
16	Payload/Cleaner Guru.app/Frameworks/Amplitude.framework/Amplitude	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/Cleaner Guru.app/Frameworks/FBLPromises.framework/FBLPromises	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/Cleaner Guru.app/Frameworks/FirebaseDynamicLinks.framework/FirebaseDynamicLinks	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/Cleaner Guru.app/Frameworks/FirebaseCrashlytics.framework/FirebaseCrashlytics	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
20	Payload/Cleaner Guru.app/Frameworks/FirebaseRemoteConfigInterop.framework/FirebaseRemoteConfigInterop	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.	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/Cleaner Guru.app/Frameworks/FirebaseCoreExtension.framework/FirebaseCoreExtension	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.	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
22	Payload/Cleaner Guru.app/Frameworks/FirebaseInstallations.framework/FirebaseInstallations	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/Cleaner Guru.app/Frameworks/AnalyticsConnector.framework/AnalyticsConnector	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
24	Payload/Cleaner Guru.app/Frameworks/SVProgressHUD.framework/SVProgressHUD	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/Cleaner Guru.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
26	Payload/Cleaner Guru.app/Frameworks/SnapKit.framework/SnapKit	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
27	Payload/Cleaner Guru.app/Frameworks/Fastis.framework/Fastis	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
28	Payload/Cleaner Guru.app/Frameworks/FirebaseCore.framework/FirebaseCore	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
29	Payload/Cleaner Guru.app/Frameworks/UITextView_Placeholder.framework/UITextView_Placeholder	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
30	Payload/Cleaner Guru.app/Frameworks/GoogleUtilities.framework/GoogleUtilities	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
31	Payload/Cleaner Guru.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

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://cleaner-970df.firebaseio.com

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
cleaner-970df.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.videolan.org	ok	**IP:** 213.36.253.2 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
crl.apple.com	ok	**IP:** 17.253.13.146 **Country:** United States of America **Region:** Florida **City:** Miami **Latitude:** 25.774269 **Longitude:** -80.193657 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ocsp.apple.com	ok	**IP:** 17.253.13.146 **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
x1cf@c.gzs o@euh.ô0kgm +@m.4h yzag@wd.164 -+-o5nodw@-epx.cq zdɛq@i e.mqc 5cщ@l.bx xr@q.kmo 44@t.n5r uy@d.këu bz@äqa.ag -@bʒ.bɼ9la2qafs ux@u.zi ljip8u@ghtv4.n lx@k.4c Ꮒ@i.2mg c@zj.k_so +ek@iyggsov.qq j@zs.esf0 я-h@v.vw m.@o.c97h giț@snᵩp1.xj xk7b@v.qřn_ m@a-.3i 8h4@i.uxw zsb@q.mq wzov@9.ie +@k.ky	

EMAIL	FILE
6@p.ma g@d.nu w@n.jj usluaa@d.zyz jv@t.lj ux9cib@0c1.7c q@ֆ.25mjâ xu@go.j9 7h@hb.hxh□n1 zq@so.mښ 6lpys@b.brq leru@uqhr3.dx yu@j.ɱfɦq bu@kt.nu î@wbc.1k z@y.kpd o@h31□g■.vyv l@w.rcv p@6.yqnӂdtv_ a4m@ȧ.sa 5ym@ć.xz h@el.dnk0s 1@o□lqcn.gpw ȝ@u.w9 qigщ@8.ẹl emt@5.su 5@3.koч5a _@2d.n6 d@pj.xm9y	Cleaner Guru.app/Cleaner Guru
h@gimv8.jx l@wyftv.3ny ƒh1iq□@w.5tf n@im9.aez	Cleaner Guru.app/Fact3Color.lottie
q@tz2ev.7e5g +u@yco.c□f 11ڰgh@rŧi.lr۔a6 d@8s7f.iծ 0@p.□d 0@rkek.vf7 fn̰@l.sow j-ʐx@□z.dh 59@k.go□_ x@ɣ.□ɣ 2n@tp.qy 7@9oi.jb sc@ʐu̧.pz e@u.n8 u@i.kg w@n.vnk	Cleaner Guru.app/widget_tutorial.mp4

EMAIL	FILE
oya06@c.jqty r@3.gc rm@i8u.ke k@v.khl 8x@ṇ5s.w2fd ʂk0sv@nzs.9s y@jyw.gv w1@q.5r -jo@ʒfcrtjj.7o	Cleaner Guru.app/Fact1.lottie
h@gimv8.jx l@wyftv.3ny n@im9.aez	Cleaner Guru.app/Fact3.lottie
nu@h.mف w_l@r.pwm	Cleaner Guru.app/splashdark.mp4
info@universeapps.limited	Cleaner Guru.app/nl.lproj/Localizable.strings
info@universeapps.limited	Cleaner Guru.app/en.lproj/Localizable.strings
info@universeapps.limitedo	Cleaner Guru.app/it.lproj/Localizable.strings
info@universeapps.limitedo	Cleaner Guru.app/es.lproj/Localizable.strings
tɗpw@v.1x r9@oi9wc.iv3z	Cleaner Guru.app/PlugIns/CleanerWidgetExtension.appex/CleanerWidgetExtension
info@universeapps.limited	Cleaner Guru.app/PlugIns/CleanerWidgetExtension.appex/nl.lproj/Localizable.strings
info@universeapps.limited	Cleaner Guru.app/PlugIns/CleanerWidgetExtension.appex/en.lproj/Localizable.strings
info@universeapps.limitedo	Cleaner Guru.app/PlugIns/CleanerWidgetExtension.appex/it.lproj/Localizable.strings
info@universeapps.limitedo	Cleaner Guru.app/PlugIns/CleanerWidgetExtension.appex/es.lproj/Localizable.strings

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
API_KEY : AIzaSyBVHBqh4eIyrkLD_TzcCdqRgsOgenKVUFs

APP STORE INFORMATION

Title: Cleaner Guru: Cleaning App

Score: 4.56344 **Features:** **Price:** 0.0 **Category:** Utilities, Business,
App Store URL: gen.universe.app.cleaner

Developer: GM UniverseApps Limited
Developer ID: 1473276099
Developer Website: https://uni.tech/en/
Developer URL: https://apps.apple.com/us/developer/gm-universeapps-limited/id1473276099?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:

Cleaner Guru is a smart application dedicated to optimizing the performance of your device by removing similar photos, merging duplicate contacts, deleting large video files, and more. It helps you to manage storage easily – a perfect solution for every mobile user. Try Cleaner Guru today to keep your iPhone running smoothly and efficiently! KEY FEATURES - Similar Photos Cleanup: Quickly detect to delete duplicate and similar photos in order to declutter your gallery. - Video Compression: Free up space by reducing video file sizes without sacrificing quality. - Contacts Cleanup: Merge duplicate contacts with one tap to tidy up your address book. - Large File Cleanup: Find and remove large files that are hogging your storage. - Widgets: Customize your home screen with widgets to monitor battery and memory usage. - Charging Animations: Personalize your charging screen with fun animations. - Secret Folder: Secure your private photos and videos with password-protected storage. HOW CLEANER GURU HELPS YOU: Optimize Performance: Clear out unnecessary files and feel your device run as smoothly as the day you got it. Free Up Space: Reclaim valuable storage space to make room for new apps, photos, and memories. Organize Your Content: Keep your photo library and contacts neat and clutter-free for easy access. Personalize Your Device: Customize your Home screen and charging experience with modern widgets and animations. Secure Your Privacy: Safeguard your personal photos and videos in a secret folder accessible only to you. SUBSCRIPTION INFORMATION Auto-Renewal: Subscriptions automatically renew unless auto-renew is turned off at least 24 hours before the end of the current period. Manage Subscriptions: You can manage subscriptions and turn off auto-renewal by going to your Account Settings after purchase. Free Trial: Any unused portion of a free trial period will be forfeited when you purchase a subscription. Payment: Payment will be charged to your iTunes Account at confirmation of purchase. Renewal Charges: Based on the selected plan, your account will be charged for renewal 24 hours before the end of the current period. JOIN OUR HAPPY MEMBERS! Millions of iPhone users have transformed their devices with Cleaner Guru. Become one of them and discover how effortless it is to keep your phone running at its best! DOWNLOAD CLEANER GURU TODAY! Download Cleaner Guru now and enjoy a cleaner, faster, and more organized iPhone experience! TERMS AND PRIVACY By using Cleaner Guru, you agree to our Terms of Service, Privacy Policy, and Billing Terms. Terms of Service: https://universeapps.limited/cleaner/tos.html Privacy Policy: https://universeapps.limited/cleaner/privacy.html Billing Terms: https://universeapps.limited/cleaner/billing.html Have any questions? Contact us via Customer Support: support@universeapps.limited

SCAN LOGS

Timestamp	Event	Error
2025-01-11 11:30:15	iOS Binary (IPA) Analysis Started	OK

2025-01-11 11:30:15	Generating Hashes	OK
2025-01-11 11:30:15	Extracting IPA	OK
2025-01-11 11:30:15	Unzipping	OK
2025-01-11 11:30:17	iOS File Analysis and Normalization	OK
2025-01-11 11:30:17	iOS Info.plist Analysis Started	OK
2025-01-11 11:30:17	Finding Info.plist in iOS Binary	OK
2025-01-11 11:30:17	Fetching Details from App Store: gen.universe.app.cleaner	OK
2025-01-11 11:30:17	Searching for secrets in plist files	OK
2025-01-11 11:30:17	Starting Binary Analysis	OK
2025-01-11 11:30:18	Dumping Classes from the binary	OK
2025-01-11 11:30:18	Running jtool against the binary for dumping classes	OK
2025-01-11 11:30:20	Library Binary Analysis Started	OK
2025-01-11 11:30:20	Framework Binary Analysis Started	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/NVActivityIndicatorView.framework/NVActivityIndicatorView	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/GoogleDataTransport.framework/GoogleDataTransport	OK

2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/PrettyCards.framework/PrettyCards	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FBAEMKit.framework/FBAEMKit	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FirebaseSessions.framework/FirebaseSessions	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/AdvancedPageControl.framework/AdvancedPageControl	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/JTAppleCalendar.framework/JTAppleCalendar	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/nanopb.framework/nanopb	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/Lottie.framework/Lottie	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/Promises.framework/Promises	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FirebaseABTesting.framework/FirebaseABTesting	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FirebaseSharedSwift.framework/FirebaseSharedSwift	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/SwiftMessages.framework/SwiftMessages	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FirebaseCoreInternal.framework/FirebaseCoreInternal	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FirebaseRemoteConfig.framework/FirebaseRemoteConfig	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/Amplitude.framework/Amplitude	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FBLPromises.framework/FBLPromises	OK

2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FirebaseDynamicLinks.framework/FirebaseDynamicLinks	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FirebaseCrashlytics.framework/FirebaseCrashlytics	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FirebaseRemoteConfigInterop.framework/FirebaseRemoteConfigInterop	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FirebaseCoreExtension.framework/FirebaseCoreExtension	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FirebaseInstallations.framework/FirebaseInstallations	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/AnalyticsConnector.framework/AnalyticsConnector	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/SVProgressHUD.framework/SVProgressHUD	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FBSDKCoreKit.framework/FBSDKCoreKit	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/SnapKit.framework/SnapKit	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/Fastis.framework/Fastis	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FirebaseCore.framework/FirebaseCore	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/UITextView_Placeholder.framework/UITextView_Placeholder	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/GoogleUtilities.framework/GoogleUtilities	OK
2025-01-11 11:30:20	Analyzing Payload/Cleaner Guru.app/Frameworks/FBSDKCoreKit_Basics.framework/FBSDKCoreKit_Basics	OK
2025-01-11 11:30:20	Extracting String Metadata	OK

2025-01-11 11:30:20	Extracting URL and Email from IPA	OK
2025-01-11 11:30:23	Performing Malware check on extracted domains	OK
2025-01-11 11:30:25	Fetching IPA icon path	OK
2025-01-11 11:30:27	Detecting Trackers from Domains	OK
2025-01-11 11:30:27	Saving to Database	OK
