IOS STATIC ANALYSIS REPORT

Cleanup (4.19.1)

File Name:	com.codeway.cleanerplus_1510944943_4.19.1.ipa
Identifier:	com.codeway.cleanerplus
Scan Date:	Jan. 11, 2025, 11:59 a.m.
App Security Score:	**43/100 (MEDIUM RISK)**

Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	7	6	0	2

FILE INFORMATION

File Name: com.codeway.cleanerplus_1510944943_4.19.1.ipa
Size: 154.7MB
MD5: 4a93242259d40e4fea32252c67f16c9d
SHA1: e166b48e12714699bbbb8e2343efcd61db2e1bbe
SHA256: 446d0a4e253b2d48d477a5f9f109360b6e9cd1f270e244651b7dc61d3f49fea0

APP INFORMATION

App Name: Cleanup
App Type: Swift

Identifier: com.codeway.cleanerplus
SDK Name: iphoneos18.1
Version: 4.19.1
Build: 50
Platform Version: 18.1
Min OS Version: 14.0
Supported Platforms: iPhoneOS,

BINARY INFORMATION

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

#CUSTOM URL SCHEMES

URL NAME	SCHEMES
com.codeway.cleanup	cleanup fb399424954414709
Editor	com.googleusercontent.apps.623140959935-hba09ii47i01f901oeo4te20cth4b37r
ReferralDynamicLinks Editor	com.codeway.cleanup

APPLICATION PERMISSIONS

PERMISSIONS	STATUS	INFO	REASON IN MANIFEST
NSCalendarsUsageDescription	dangerous	Access Calendars.	We may need an access to calendar for ad content
NSCameraUsageDescription	dangerous	Access the Camera.	Cleanup needs access to your camera so you can start taking photos and videos to save them in your Secret Space
NSContactsUsageDescription	dangerous	Access Contacts.	We need an access to your contact list
NSFaceIDUsageDescription	normal	Access the ability to authenticate with Face ID.	We need an access to your Face ID
NSLocationWhenInUseUsageDescription	dangerous	Access location information when app is in the foreground.	We need an access to your location for app improvement
NSMicrophoneUsageDescription	dangerous	Access microphone.	We need an access to your mic
NSPhotoLibraryUsageDescription	dangerous	Access the user's photo library.	We need an access to your photo gallery for photo scanning

APP TRANSPORT SECURITY (ATS)

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	NSExceptionDomains	info	admost.com
2	Insecure communication to admost.com is allowed	high	NSExceptionAllowsInsecureHTTPLoads allows insecure HTTP loads to admost.com, or to be able to loosen the server trust evaluation requirements for HTTPS connections to the domain.
3	NSIncludesSubdomains set to TRUE for admost.com	info	NSIncludesSubdomains applies the ATS exceptions for the given domain to all subdomains as well. For example, the ATS exceptions in the domain exception dictionary apply to admost.com, as well as math.admost.com, history.admost.com, and so on. Otherwise, if the value is NO, the exceptions apply only to admost.com.
4	NSRequiresCertificateTransparency set to NO for admost.com	warning	Certificate Transparency (CT) is a protocol that ATS can use to identify mistakenly or maliciously issued X.509 certificates. Set the value for the NSRequiresCertificateTransparency key to YES to require that for a given domain, server certificates are supported by valid, signed CT timestamps from at least two CT logs trusted by Apple. This key is optional. The default value is NO.

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 , _sscanf , _strlen , _strncpy
2	Binary makes use of the insecure Random function(s)	warning	**CWE:** CWE-330: Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6	The binary may use the following insecure Random function(s) _srand
3	Binary makes use of Logging function	info	**CWE:** CWE-532: Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3	The binary may use _NSLog function for logging.
4	Binary makes use of malloc function	warning	**CWE:** CWE-789: Uncontrolled Memory Allocation **OWASP Top 10:** M7: Client Code Quality **OWASP MASVS:** MSTG-CODE-8	The binary may use _malloc function instead of calloc

IPA BINARY ANALYSIS

PROTECTION	STATUS	SEVERITY	DESCRIPTION
NX	False	info	The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.
PIE	True	info	The binary is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.
STACK CANARY	True	info	This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.
ARC	True	info	The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.

PROTECTION	STATUS	SEVERITY	DESCRIPTION
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	True	info	Debug Symbols are stripped

DYNAMIC LIBRARY & FRAMEWORK BINARY ANALYSIS

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
1	Frameworks/libswift_Concurrency.dylib	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.	False warning This binary is not encrypted.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
1	Payload/Clean-Gallery.app/Frameworks/RxCocoa.framework/RxCocoa	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.	F w D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
2	Payload/Clean-Gallery.app/Frameworks/VHGradientView.framework/VHGradientView	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.	F w D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
3	Payload/Clean-Gallery.app/Frameworks/Kingfisher.framework/Kingfisher	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.	F w D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED
4	Payload/Clean-Gallery.app/Frameworks/Differentiator.framework/Differentiator	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
5	Payload/Clean-Gallery.app/Frameworks/FBSDKLoginKit.framework/FBSDKLoginKit	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED
6	Payload/Clean-Gallery.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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
7	Payload/Clean-Gallery.app/Frameworks/SwiftUIIntrospect_2C5EC2718B657AE7_PackageProduct.framework/SwiftUIIntrospect_2C5EC2718B657AE7_PackageProduct	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
8	Payload/Clean-Gallery.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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED
9	Payload/Clean-Gallery.app/Frameworks/ActiveLabel.framework/ActiveLabel	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
10	Payload/Clean-Gallery.app/Frameworks/SwiftyRSA.framework/SwiftyRSA	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.	F w D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
11	Payload/Clean-Gallery.app/Frameworks/Moya_64575493A_PackageProduct.framework/Moya_64575493A_PackageProduct	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED
12	Payload/Clean-Gallery.app/Frameworks/SwiftRichString.framework/SwiftRichString	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
13	Payload/Clean-Gallery.app/Frameworks/FacebookBasics_-72B781E718BFD883_PackageProduct.framework/FacebookBasics_-72B781E718BFD883_PackageProduct	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED
14	Payload/Clean-Gallery.app/Frameworks/WidgetUI.framework/WidgetUI	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
15	Payload/Clean-Gallery.app/Frameworks/RxRelay.framework/RxRelay	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.	F w D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
16	Payload/Clean-Gallery.app/Frameworks/CocoaImageHashing.framework/CocoaImageHashing	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
17	Payload/Clean-Gallery.app/Frameworks/Kronos.framework/Kronos	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.	F w D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
18	Payload/Clean-Gallery.app/Frameworks/Mute.framework/Mute	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.	F v D S a s c s S S D Y D F t S F i b

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

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED
20	Payload/Clean-Gallery.app/Frameworks/UI.framework/UI	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
21	Payload/Clean-Gallery.app/Frameworks/FacebookLogin_-28D52AF5BD2BF5E0_PackageProduct.framework/FacebookLogin_-28D52AF5BD2BF5E0_PackageProduct	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
22	Payload/Clean-Gallery.app/Frameworks/CerebroCoreKit_-2C6AF4AEEDCB3D7F_PackageProduct.framework/CerebroCoreKit_-2C6AF4AEEDCB3D7F_PackageProduct	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.	F w D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
23	Payload/Clean-Gallery.app/Frameworks/NSObject_Rx.framework/NSObject_Rx	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
24	Payload/Clean-Gallery.app/Frameworks/ADMozaicCollectionViewLayout.framework/ADMozaicCollectionViewLayout	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED
25	Payload/Clean-Gallery.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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED
26	Payload/Clean-Gallery.app/Frameworks/CWNetworkKit_-723357F909649548_PackageProduct.framework/CWNetworkKit_-723357F909649548_PackageProduct	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.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
27	Payload/Clean-Gallery.app/Frameworks/UIScrollView_InfiniteScroll.framework/UIScrollView_InfiniteScroll	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
28	Payload/Clean-Gallery.app/Frameworks/RxDataSources.framework/RxDataSources	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
29	Payload/Clean-Gallery.app/Frameworks/FBSDKShareKit.framework/FBSDKShareKit	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
30	Payload/Clean-Gallery.app/Frameworks/Adjust_171B82C01A32B1_PackageProduct.framework/Adjust_171B82C01A32B1_PackageProduct	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
31	Payload/Clean-Gallery.app/Frameworks/FacebookAEM.framework/FacebookAEM	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.	F w D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
32	Payload/Clean-Gallery.app/Frameworks/FacebookCore.framework/FacebookCore	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.	F w D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
33	Payload/Clean-Gallery.app/Frameworks/PromiseKit.framework/PromiseKit	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
34	Payload/Clean-Gallery.app/Frameworks/Core.framework/Core	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.	F w D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
35	Payload/Clean-Gallery.app/Frameworks/Alamofire_-213FC01918BCE467_PackageProduct.framework/Alamofire_-213FC01918BCE467_PackageProduct	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.	F w D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
36	Payload/Clean-Gallery.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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
37	Payload/Clean-Gallery.app/Frameworks/FacebookShare_-28D4484CC79DB1E6_PackageProduct.framework/FacebookShare_-28D4484CC79DB1E6_PackageProduct	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	S S
38	Payload/Clean-Gallery.app/Frameworks/ThemeHelper.framework/ThemeHelper	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.	F v D S a s c s S S D Y D F t S F i b

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED
39	Payload/Clean-Gallery.app/Frameworks/RxSwift.framework/RxSwift	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.

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://cleanerplus-dev.firebaseio.com
App talks to a Firebase database	info	The app talks to Firebase database at https://cleanerplus-staging.firebaseio.com
App talks to a Firebase database	info	The app talks to Firebase database at https://cleanerplus.firebaseio.com

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
consent.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
invite-dev.cleanup.photos	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
consent.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
cleanerplus-staging.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
static-cdn-production.cleanerapi.com	ok	**IP:** 34.120.167.27 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
consent.adjust.net.in	ok	**IP:** 185.151.204.31 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
invite.cleanup.photos	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
support.apple.com	ok	**IP:** 184.84.132.142 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.363598 **Longitude:** -71.085205 **View:** Google Map
crl.apple.com	ok	**IP:** 17.253.13.145 **Country:** United States of America **Region:** Florida **City:** Miami **Latitude:** 25.774269 **Longitude:** -80.193657 **View:** Google Map
ocsp.apple.com	ok	**IP:** 17.253.13.136 **Country:** United States of America **Region:** Florida **City:** Miami **Latitude:** 25.774269 **Longitude:** -80.193657 **View:** Google Map
consent.adjust.com	ok	**IP:** 185.151.204.203 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
cleanerplus.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
certs.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

DOMAIN	STATUS	GEOLOCATION
consent.adjust.cn	ok	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
consent.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
www.apple.com	ok	**IP:** 23.37.124.29 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
consent.tr.adjust.com	ok	**IP:** 195.244.54.7 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
consent.adjust.world	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
cleanerplus-dev.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
invite-staging.cleanup.photos	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
6@w6m.f6 6@5.5m	Clean-Gallery.app/facenet_int_quantized.tflite
ν_@zet2.ŗg	Clean-Gallery.app/SF-Pro-Display-Bold.otf
a@lm.latu4k a@hӟwʕn.lau xc@b.fyپhd s@hu.atp o@s.zb0m yww@m4nr.ɟ8 zqsvh@tgq4.lq zo@שnzگ.oȍrd o□v@d.no_1 .@pprgv.bje 7@r.syk p@rxv.fzkhca ے@ʆ.pj q@b7r.ǽ5 ·@w.oaz m@-ml.ï2 a@e.iod nzp@f.nbĵd v@d._y p2b1@4.kl t@gdcr.qou□ r@m.mxъr v@wquvaas.gbr ɋ@i.ifv k@7-.űc fj@i.5ös u6l@k.d3 sm@c.□t 7.bg@twc.vtpb qpf@йr.yc 5u@□a._2l x@uuv.etl b@ȿ.ӎd c@wvz.gw r@8.w8 _bđ@7.k3zbt m@b.lx w6uk@c.hid a@w.dt 8@d.xs 2@1.ȝ5cr f@r3v.yꟻ 8@d.3kmt µ5f@5.dh um@8v.cķ xsl□wt4@z.yn mpnuj@k.vjgf qm@7.zs e@mq.ﻫx u@u.zʌp i@p.a9sd	Clean-Gallery.app/Clean-Gallery

EMAIL	FILE
3@o.214 8@8.ƨ0 o9иvy@и.bx 60@1.aƞ9364 c@x.l2w	Clean-Gallery.app/face_detection.tflite
ν_@zet2.ɼg	Clean-Gallery.app/PlugIns/BatteryStorageWidgetExtension.appex/SF-Pro-Display-Bold.otf
4@z.yn 8@d.3km	IPA Strings Dump
+@l.d_	Payload/Clean-Gallery.app/Frameworks/Lottie.framework/Lottie
p@_t.dco f@5y.uvwwk 8@f7.az i@9j.km e@o.kv	Payload/Clean-Gallery.app/Frameworks/Core.framework/Core

TRACKERS

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

HARDCODED SECRETS

POSSIBLE SECRETS
FacebookClientToken : 0c9262f5b0591c29417244dd6879cf22
API_KEY : AIzaSyCwFtS4GiegiepRHemcMNgxm8CZ4vKeY5I
API_KEY : AIzaSyA6z-nyn7EhBYqRFImDiiJuMaMdyNE6GmY
token : tyk0f9rqwydc
API_KEY : AIzaSyAN0uiFePtKpQ-Lft5Jz6LstvuEJH9CX9w

APP STORE INFORMATION

Title: Cleanup: Phone Storage Cleaner

Score: 4.69789 **Features: Price:** 0.0 **Category:** Utilities, Photo & Video,
App Store URL: com.codeway.cleanerplus

Developer: Codeway Dijital Hizmetler Anonim Sirketi

Developer ID: 1503508447
Developer Website: https://codeway.co
Developer URL: https://apps.apple.com/us/developer/codeway-dijital-hizmetler-anonim-sirketi/id1503508447?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:

LET'S FACE IT: CLEANING UP YOUR PHOTO LIBRARY IS SO BORING! Cleanup is here to make this process easy, fun & safe. CLEAN UP YOUR GALLERY IN NO TIME Swipe left — to get rid of unwanted photos/duplicates Swipe right — to keep the memories that actually matter to you You'll be surprised to see how many unnecessary photos you've been keeping in your gallery! ONLY KEEP THE BEST PHOTOS In a bunch of similar photos, Cleanup will suggest to you which one to keep Cleanup will suggest to you the photo that... ... you're directly looking at the camera ... you're smiling ... has a good focus ... you edited or favorited in the past Still, you decide on which one to keep, we don't delete any photos without your permission. YOU HAVE THE FINAL WORD Think of the Trash folder in your computer, Cleanup has exactly the same. After you're done with deleting, Cleanup asks you to do a final review; so that you don't delete any photos by accident. RELIEVE STRESS WHILE STAYING PRODUCTIVE Honestly, we're now pretty sure that our biggest competitors are cute kittens, pimple-popping videos, or your favorite puzzle game. But here's what's unique to Cleanup: After you spend some time on our app, what you get is a clean & organized photo gallery - not a guilt-provoking waste of time! MOST SECURE WAY TO CLEAN UP YOUR LIBRARY Unlike other apps, you don't need an internet connection to use Cleanup. Cleanup works locally (offline) on your phone, so we couldn't misuse your photos even if we wanted to :) SORT VIDEOS BY SIZE - DELETE THE LARGEST ONE FIRST Easily start with that 2GB video that's been sitting in your gallery for a long time. Payment & Subscription Terms: Choose between the following subscription options for unlimited access to all features: • Weekly Subscription • Lifetime Subscription FREE TRIAL FOR 7 DAYS - OFFERING UNLIMITED GALLERY CLEANING FOR A LIMITED TIME ***You may cancel your subscription at any time*** Cleanup's free trial allows you unlimited access to all features for the duration of 7 days. Your account will be automatically charged for renewal, based on the annual subscription plan, within 24 hours before the end of the 7 days free trial period. You can cancel auto-renewal at any time, given that the cancellation is at least 24 hours before the end of the current period. Any unused portion of a free trial period will be forfeited when making a purchase of an auto-renewing subscription. ***Manage your subscription directly from your iPhone*** Subscriptions can be managed by the user and auto-renewal can be turned off by going to the Account Settings: - Open the Settings app. - Tap your name. - Tap Subscriptions. - Tap the subscription that you want to manage. Privacy policy: https://cleanup.photos/privacy Terms of use: https://cleanup.photos/terms

SCAN LOGS

Timestamp	Event	Error
2025-01-11 11:59:59	iOS Binary (IPA) Analysis Started	OK
2025-01-11 11:59:59	Generating Hashes	OK
2025-01-11 11:59:59	Extracting IPA	OK
2025-01-11 11:59:59	Unzipping	OK
2025-01-11 12:00:00	iOS File Analysis and Normalization	OK
2025-01-11 12:00:00	iOS Info.plist Analysis Started	OK
2025-01-11 12:00:00	Finding Info.plist in iOS Binary	OK

2025-01-11 12:00:00	Fetching Details from App Store: com.codeway.cleanerplus	OK
2025-01-11 12:00:01	Searching for secrets in plist files	OK
2025-01-11 12:00:01	Starting Binary Analysis	OK
2025-01-11 12:00:01	Dumping Classes from the binary	OK
2025-01-11 12:00:01	Running jtool against the binary for dumping classes	OK
2025-01-11 12:00:02	Library Binary Analysis Started	OK
2025-01-11 12:00:02	Analyzing Payload/Clean-Gallery.app/Frameworks/libswift_Concurrency.dylib	OK
2025-01-11 12:00:02	Framework Binary Analysis Started	OK
2025-01-11 12:00:02	Analyzing Payload/Clean-Gallery.app/Frameworks/RxCocoa.framework/RxCocoa	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/VHGradientView.framework/VHGradientView	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/Kingfisher.framework/Kingfisher	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/Differentiator.framework/Differentiator	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/FBSDKLoginKit.framework/FBSDKLoginKit	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/FBAEMKit.framework/FBAEMKit	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/SwiftUIIntrospect_2C5EC2718B657AE7_PackageProduct.framework/SwiftUIIntrospect_2C5EC2718B657AE7_PackageProduct	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/Lottie.framework/Lottie	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/ActiveLabel.framework/ActiveLabel	OK

2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/SwiftyRSA.framework/SwiftyRSA	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/Moya_64575493A_PackageProduct.framework/Moya_64575493A_PackageProduct	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/SwiftRichString.framework/SwiftRichString	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/FacebookBasics_-72B781E718BFD883_PackageProduct.framework/FacebookBasics_-72B781E718BFD883_PackageProduct	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/WidgetUI.framework/WidgetUI	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/RxRelay.framework/RxRelay	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/CocoaImageHashing.framework/CocoaImageHashing	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/Kronos.framework/Kronos	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/Mute.framework/Mute	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/AdjustSigSdk.framework/AdjustSigSdk	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/UI.framework/UI	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/FacebookLogin_-28D52AF5BD2BF5E0_PackageProduct.framework/FacebookLogin_-28D52AF5BD2BF5E0_PackageProduct	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/CerebroCoreKit_-2C6AF4AEEDCB3D7F_PackageProduct.framework/CerebroCoreKit_-2C6AF4AEEDCB3D7F_PackageProduct	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/NSObject_Rx.framework/NSObject_Rx	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/ADMozaicCollectionViewLayout.framework/ADMozaicCollectionViewLayout	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/FBSDKCoreKit.framework/FBSDKCoreKit	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/CWNetworkKit_-723357F909649548_PackageProduct.framework/CWNetworkKit_-723357F909649548_PackageProduct	OK

2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/UIScrollView_InfiniteScroll.framework/UIScrollView_InfiniteScroll	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/RxDataSources.framework/RxDataSources	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/FBSDKShareKit.framework/FBSDKShareKit	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/Adjust_171B82C01A32B1_PackageProduct.framework/Adjust_171B82C01A32B1_PackageProduct	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/FacebookAEM.framework/FacebookAEM	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/FacebookCore.framework/FacebookCore	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/PromiseKit.framework/PromiseKit	OK
2025-01-11 12:00:03	Analyzing Payload/Clean-Gallery.app/Frameworks/Core.framework/Core	OK
2025-01-11 12:00:16	Analyzing Payload/Clean-Gallery.app/Frameworks/Alamofire_-213FC01918BCE467_PackageProduct.framework/Alamofire_-213FC01918BCE467_PackageProduct	OK
2025-01-11 12:00:16	Analyzing Payload/Clean-Gallery.app/Frameworks/FBSDKCoreKit_Basics.framework/FBSDKCoreKit_Basics	OK
2025-01-11 12:00:16	Analyzing Payload/Clean-Gallery.app/Frameworks/FacebookShare_-28D4484CC79DB1E6_PackageProduct.framework/FacebookShare_-28D4484CC79DB1E6_PackageProduct	OK
2025-01-11 12:00:17	Analyzing Payload/Clean-Gallery.app/Frameworks/ThemeHelper.framework/ThemeHelper	OK
2025-01-11 12:00:17	Analyzing Payload/Clean-Gallery.app/Frameworks/RxSwift.framework/RxSwift	OK
2025-01-11 12:00:17	Extracting String Metadata	OK
2025-01-11 12:00:17	Extracting URL and Email from IPA	OK
2025-01-11 12:00:23	Performing Malware check on extracted domains	OK
2025-01-11 12:00:26	Fetching IPA icon path	OK

2025-01-11 12:00:28	Detecting Trackers from Domains	OK
2025-01-11 12:00:28	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.