

ANDROID STATIC ANALYSIS REPORT

((•))

Tether companion (0.2)

File Name:	installer99.apk
Package Name:	rino.org.tethercompanion
Scan Date:	May 31, 2022, 9:11 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	♥ HOTSPOT
2	3	1	2	0

FILE INFORMATION

File Name: installer99.apk

Size: 1.15MB

MD5: a414326a998a750abda4cc3f3d8b5ec8

SHA1: 142945afed883194b8f9f61aab5896214e76b1eb

SHA256: a09d91d7beb340f0bf6e6b048469315cc019be0a9897c23d89ac5d22ec3333ff

i APP INFORMATION

App Name: Tether companion

Package Name: rino.org.tethercompanion

Main Activity: rino.org.tethercompanion.MainActivity

Target SDK: 23 Min SDK: 15 Max SDK:

Android Version Name: 0.2 Android Version Code: 2

EE APP COMPONENTS

Activities: 1 Services: 1 Receivers: 0 Providers: 0

Exported Activities: O Exported Services: 1 Exported Receivers: O Exported Providers: O



APK is signed v1 signature: True v2 signature: False v3 signature: False

Found 1 unique certificates

Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2015-12-30 07:42:03+00:00 Valid To: 2043-05-17 07:42:03+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x3d2def9d Hash Algorithm: sha256

md5: 83a4295c02cb434a028e0a16f21d1ad8

sha1: 30025ad629e026190725057389b890ed311214a8

sha256: 629d6109cd091eb8521189395479fe40a70d1fccc9da8ab351ed9338c8e69867

sha512: 4aaf14137e07e0c4c03a054edc9505b3fe6108e2aa9bf8dec1914625999bd8c9355c45b8f9c3aecac0f58065ff2690dc698db6898908ab3c2d62c5a67948a132abbf8dec1914625999bd8c9355c45b8f9c3aecac0f58065ff2690dc698db6898908ab3c2d62c5a67948a132abbf8dec1914625999bd8c9355c45b8f9c3aecac0f58065ff2690dc698db6898908ab3c2d62c5a67948a132abbf8dec1914625999bd8c9355c45b8f9c3aecac0f58065ff2690dc698db6898908ab3c2d62c5a67948a132abbf8dec1914625999bd8c9355c45b8f9c3aecac0f58065ff2690dc698db6898908ab3c2d62c5a67948a132abbf8dec1914625999bd8c9355c45b8f9c3aecac0f58065ff2690dc698db6898908ab3c2d62c5a67948a132abbf8dec1914625999bd8c9355c45b8f9c3aecac0f58065ff2690dc698db6898908ab3c2d62c5a67948a132abbf8dec1914625999bd8c9355c45b8f9c3aecac0f58065ff2690dc698db6898908ab3c2d62c5a67948a132abbf8dec1914625999bd8c9355c45b8f9c3aecac0f58065b8f9c3aecac0ff58065b8f9c465b8f9c465b8f9c465b8f9c465b8f9c465b8f9c465b8f9c465b8f9c465b8f9c465b8f9c465b8f9c465b8f9c465b8f9c465b8f9c465b8f9c465b8f9c465b8f

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

M APKID ANALYSIS

FILE	DETAILS				
	FINDINGS	DETAILS			
classes.dex	Compiler	dx (possible dexmerge)			
	Manipulator Found	dexmerge			

△ NETWORK SECURITY

NO SCOPE SEVERITY DESCRIPTION

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
2	Service (rino.org.tethercompanion.WebServerService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	rino/org/tethercompanion/MyHttpServ er.java rino/org/tethercompanion/MainActivity .java fi/iki/elonen/SimpleWebServer.java fi/iki/elonen/util/ServerRunner.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	fi/iki/elonen/NanoHTTPD.java
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	fi/iki/elonen/NanoHTTPD.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	fi/iki/elonen/NanoHTTPD.java

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
7	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
8	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
9	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
clients3.google.com	ok	IP: 142.251.39.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.paypal.me	ok	IP: 151.101.129.21 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

Report Generated by - MobSF v3.5.2 Beta

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.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.