

ANDROID STATIC ANALYSIS REPORT



Moonlight (9.7.7)

File Name:	installer108.apk
Package Name:	com.limelight
Scan Date:	May 31, 2022, 12:55 p.m.
App Security Score:	42/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
5	8	1	2	1

FILE INFORMATION

File Name: installer108.apk

Size: 5.22MB

MD5: bd6ee602a799b3af4cb1dd67300ec997

SHA1: 2c0ddada2cda76ed096b144bc8d361c1fdccde32

SHA256: 37d26e206de7da32ce28fc6c897bd226e2c55a945ad6b4e2606a7fa011b94fd9

i APP INFORMATION

App Name: Moonlight

Package Name: com.limelight

Main Activity: com.limelight.PcView

Target SDK: 30 Min SDK: 16 Max SDK:

Android Version Name: 9.7.7
Android Version Code: 247

B APP COMPONENTS

Activities: 7
Services: 3
Receivers: 0
Providers: 1

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

***** CERTIFICATE INFORMATION

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

Found 1 unique certificates

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

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2019-07-16 08:14:57+00:00 Valid To: 2046-12-01 08:14:57+00:00

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

Serial Number: 0x6f895317 Hash Algorithm: sha256

md5: 63a8b8988efbf9d342b9e8ec275a91d5

sha1: 165c5f231ae5fd90e72813acd547ddf801696b88

sha256: e781cffbd6737c4e4ac471a1d24762626b139a19ac87131354d2c6ea9b03c72a

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 0253b272f6a1eb10d05131c483b7e1993b6115ec82880a70d3e473bbb9cf4e41

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.android.providers.tv.permission.READ_EPG_DATA	unknown	Unknown permission	Unknown permission from android reference
com.android.providers.tv.permission.WRITE_EPG_DATA	unknown	Unknown permission	Unknown permission from android reference

M APKID ANALYSIS

FILE	DETAILS					
classes.dex	FINDINGS	DETAILS				
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check				
	Compiler	r8				



NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
2	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.
3	Content Provider (com.limelight.PosterContentProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.limelight.ShortcutTrampoline) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Launch Mode of Activity (com.limelight.Game) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/limelight/grid/AppGridAdapter.jav a com/limelight/computers/ComputerMa nagerService.java com/limelight/binding/input/virtual_co ntroller/VirtualControllerElement.java com/limelight/binding/input/driver/Usb DriverService.java com/limelight/nvstream/mdns/MdnsDi scoveryAgent.java com/limelight/binding/input/driver/Abs tractXboxController.java com/limelight/nvstream/wol/WakeOnL anSender.java com/limelight/grid/assets/NetworkAsse tLoader.java com/limelight/binding/video/MediaCod ecHelper.java com/limelight/binding/input/driver/Xbo x360Controller.java com/limelight/binding/input/driver/Xbo x360Controller.java com/limelight/binding/input/driver/Xbo
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	com/limelight/AppView.java com/limelight/Game.java com/limelight/binding/audio/AndroidA udioRenderer.java com/limelight/grid/assets/MemoryAsse tLoader.java com/limelight/binding/crypto/AndroidC ryptoProvider.java com/limelight/nvstream/NvConnection. java com/limelight/nvstream/http/PairingMa

NO	ISSUE	SEVERITY	STANDARDS	com/limelight/binding/input/Controller
				com/limelight/binding/input/driver/Xbo xOneController.java com/limelight/binding/input/capture/In putCaptureManager.java com/limelight/grid/assets/DiskAssetLoa der.java com/limelight/nvstream/http/NvApp.jav a com/limelight/computers/IdentityMana ger.java com/limelight/nvstream/http/NvHTTP.j ava com/limelight/computers/LegacyDatab aseReader.java com/limelight/preferences/StreamSettin gs.java com/limelight/binding/video/MediaCod ecDecoderRenderer.java org/slf4j/helpers/Util.java com/limelight/PcView.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/limelight/nvstream/wol/WakeOnL anSender.java javax/jmdns/impl/JmDNSImpl.java
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/limelight/computers/LegacyDatab aseReader2.java com/limelight/computers/ComputerDat abaseManager.java com/limelight/computers/LegacyDatab aseReader.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	com/limelight/nvstream/http/PairingMa nager.java
5	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/limelight/nvstream/http/PairingMa nager.java
6	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/limelight/nvstream/http/PairingMa nager.java
7	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/limelight/computers/ldentityMana ger.java javax/jmdns/impl/JmDNSImpl.java javax/jmdns/impl/DNSRecord.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/limelight/nvstream/http/NvHTTP.j ava



NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi- v7a/libmoonlight-core.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object 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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/x86/libmoonlight-core.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object 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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/arm64-v8a/libmoonlight- core.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object 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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['memcpy_chk', 'FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/x86_64/libmoonlight- core.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object 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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['memcpy_chk', 'FD_SET_chk']	True info Symbols are stripped.

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'USB'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	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.
8	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.
9	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(3),FCS_CKM.1.2(3)	Selection-Based Security Functional Requirements	Password Conditioning	A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption not in accordance with FCS_COP.1.1(1), AES-ECB mode is being used.
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.
14	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
15	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
16	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
17	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
18	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The application validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates', 'The application validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 2560 or a Certificate Revocation List (CRL) as specified in RFC 5759 or an OCSP TLS Status Request Extension (i.e., OCSP stapling) as specified in RFC 6066', 'The certificate path must terminate with a trusted CA certificate'].
19	FIA_X509_EXT.1.2	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.
20	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
21	FIA_X509_EXT.2.2	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	When the application cannot establish a connection to determine the validity of a certificate, the application allow the administrator to choose whether to accept the certificate in these cases or accept the certificate, or not accept the certificate.
22	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	IP: 83.166.144.67 Country: Switzerland Region: Geneve City: Carouge Latitude: 46.180962 Longitude: 6.139210 View: Google Map
github.com	ok	IP: 140.82.121.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
schemas.moonlight-stream.com	ok	No Geolocation information available.
schemas.android.com	ok	No Geolocation information available.

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.