

ANDROID STATIC ANALYSIS REPORT



♠ MyNM (2.3.0)

File Name:	org.nm.mobile.myNM_1729266435.apk
Package Name:	org.nm.mobile.myNM
Scan Date:	Aug. 28, 2025, 10:07 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	® HOTSPOT
3	18	3	4	2

FILE INFORMATION

File Name: org.nm.mobile.myNM_1729266435.apk

Size: 72.71MB

MD5: 86142f142d4d104fddcc96bbb5329387

SHA1: 953fd16fb9425d7cae1cbd183ffdfbbb7817f79b

SHA256: 7caa51d06caa4d067394f2f2a7e13d50dd672b3dc0f8e3b3ae5649b563c2323a

i APP INFORMATION

App Name: MyNM

Package Name: org.nm.mobile.myNM

Main Activity: org.nm.mynm.v1.base.SplashActivity

Target SDK: 34 Min SDK: 29 Max SDK:

Android Version Name: 2.3.0 Android Version Code: 1729266435

B APP COMPONENTS

Activities: 143 Services: 13 Receivers: 6 Providers: 3

Exported Activities: 4
Exported Services: 2
Exported Receivers: 2
Exported Providers: 0

***** CERTIFICATE INFORMATION

Binary is signed v1 signature: False v2 signature: True v3 signature: False v4 signature: False

X.509 Subject: C=01, ST=IL, L=Chicago, O=Northwestern Medicine, OU=NMIT, CN=Northwestern Medicine

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2018-11-15 08:03:37+00:00 Valid To: 2043-11-09 08:03:37+00:00

Issuer: C=01, ST=IL, L=Chicago, O=Northwestern Medicine, OU=NMIT, CN=Northwestern Medicine

Serial Number: 0x3cf404dc Hash Algorithm: sha256

md5: 6e1f0f6410e1589b0d1c4ee3a7aa9d4e

sha1: fdfc9222f5297dc324bbb08eafc84606c261f85d

sha256: 7bcec1366776fdd90e326acae8a80e69f81ba4f63b7e019017c45d433d58d3a9

sha512: 05af9d37e4681580c2779216dc5897369cff4ef27a08e73edb2a57bb4fbd65c377f8ae5465eeafb398050941e402e53d505cf206526b4eea50a2597502be8eb3

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: f5e71bfd5d5b5af115262080164cb937116379ec75705acf797c9fd9ae4abb45

Found 1 unique certificates

E APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE		read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network- based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH.SCAN		Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.hardware.place.gps	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.CAMERA		take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.SCHEDULE_EXACT_ALARM		permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
org.nm.mobile.myNM.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

M APKID ANALYSIS

FILE	DETAILS		
	FINDINGS	DETAILS	
	yara_issue	yara issue - dex file recognized by apkid but not yara module	
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check	
	Compiler	unknown (please file detection issue!)	
	FINDINGS	DETAILS	
classes2.dex	yara_issue	yara issue - dex file recognized by apkid but not yara module	
	Compiler	unknown (please file detection issue!)	

FILE	DETAILS			
	FINDINGS	DETAILS		
	yara_issue	yara issue - dex file recognized by apkid but not yara module		
classes3.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check		
	Compiler	unknown (please file detection issue!)		
	FINDINGS	DETAILS		
classes4.dex	yara_issue	yara issue - dex file recognized by apkid but not yara module		
	Compiler	unknown (please file detection issue!)		

FILE	DETAILS			
	FINDINGS	DETAILS		
	yara_issue	yara issue - dex file recognized by apkid but not yara module		
classes5.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check		
	Compiler	unknown (please file detection issue!)		
	FINIDINGS	DETAILC		
	FINDINGS	DETAILS		
	yara_issue	yara issue - dex file recognized by apkid but not yara module		
classes6.dex	Anti-VM Code	Build.MANUFACTURER check Build.TAGS check		
	Compiler	unknown (please file detection issue!)		

■ BROWSABLE ACTIVITIES

ACTIVITY INTENT		
-----------------	--	--

ACTIVITY	INTENT
org.nm.mynm.v1.base.DeeplinkIntermediateActivity	Schemes: https://, Hosts: mobile.nm.org, Path Prefixes: /, Path Patterns: /.*,
epic.mychart.android.library.prelogin.SplashActivity	Schemes: epicmychart://,

△ NETWORK SECURITY

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

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.
3	*	high	Base config is configured to trust user installed certificates.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

Q MANIFEST ANALYSIS

HIGH: 0 | WARNING: 8 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/wp_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	Activity (org.nm.mynm.v1.base.DeeplinkIntermediateActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Activity (epic.mychart.android.library.prelogin.SplashActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (epic.mychart.android.library.healthlinks.HealthConnectPrivacyPolicyActivity) is not Protected. [android:exported=true]	warning	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	Activity-Alias (epic.mychart.android.library.HealthConnectViewPermissionsActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.START_VIEW_PERMISSION_USAGE [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 8 | INFO: 1 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/e.java com/bumptech/glide/load/engine/d.java com/bumptech/glide/load/engine/o.java com/bumptech/glide/load/engine/w.java com/bumptech/glide/manager/l.java com/epic/patientengagement/authentication/login/activit ies/PreloginInternalWebViewActivity.java com/epic/patientengagement/authentication/login/activit ies/PreloginInternalWebViewFragment.java com/epic/patientengagement/authentication/login/activit ies/SAMLLoginActivity.java com/epic/patientengagement/authentication/login/fragm ents/EnterPasscodeDialogFragment.java com/epic/patientengagement/authentication/login/fragm ents/LoginFragment.java com/epic/patientengagement/authentication/login/fragm

NO	ISSUE	SEVERITY	STANDARDS	ents/LongTextDialogFragment.java FoliFe pic/patientengagement/authentication/login/fragments/OrgFragment.java
1	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/epic/patientengagement/authentication/login/utilities/LoginHelper.java com/epic/patientengagement/authentication/login/utilities/LoginResultCode.java com/epic/patientengagement/authentication/login/utilities/OrganizationLoginHelper.java com/epic/patientengagement/authentication/login/utilities/SamlSessionManager.java com/epic/patientengagement/core/component/lAuthenticationComponentAPI.java com/epic/patientengagement/core/deeplink/DeepLinkLaunchParameters.java com/epic/patientengagement/core/mychartweb/External JumpDialogFragment.java com/epic/patientengagement/core/mychartweb/MyChartWebQueryParameters.java com/epic/patientengagement/core/mychartweb/MyChartWebViewClient.java com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java com/epic/patientengagement/core/mychartweb/WebSessionWebServiceAPI.java com/epic/patientengagement/core/onboarding/OnboardingHostFragment.java com/epic/patientengagement/core/onboarding/OnboardingPageFragment.java com/epic/patientengagement/core/permissions/PermissionProminentDisclosure.java com/epic/patientengagement/core/utilities/PrintUtil.java com/epic/patientengagement/core/utilities/PrintUtil.java com/epic/patientengagement/core/utilities/WebUtil.java com/epic/patientengagement/core/utilities/WebUtil.java com/epic/patientengagement/core/utilities/WebUtil.java com/epic/patientengagement/core/utilities/PrintUtil.java com/epic/patientengagement/core/utilities/PrintUtil.java com/epic/patientengagement/core/utilities/WebUtil.java com/epic/patientengagement/core/utilities/PrintUtil.java com/epic/patientengagement/core/utilities/WebUtil.java com/epic/patientengagement/core/utilities/PrintUtil.java com/epic/patientengagement/core/webservice/WebService.java com/epic/patientengagement/core/webservice/Processo r/MyChartResponseProcessor.java

NO	ISSUE	SEVERITY	STANDARDS	com/epic/patientengagement/homepage/HomePageCom FUNESTAPI.java epic/mychart/android/library/api/classes/WPAPIAuthenti
				cation.java
				epic/mychart/android/library/healthlinks/d.java
				org/nm/mynm/v2/ui/healthbeat/view/HealthBeatActivity
				.java
				org/nm/mynm/v2/ui/mytools/view/MyToolsActivity.java
				com/airbnb/lottie/LottieAnimationView.java
				com/airbnb/lottie/utils/c.java
				com/bumptech/glide/b.java
				com/bumptech/glide/disklrucache/a.java
				com/bumptech/glide/gifdecoder/d.java
				com/bumptech/glide/gifdecoder/e.java
				com/bumptech/glide/load/data/b.java
				com/bumptech/glide/load/data/j.java
				com/bumptech/glide/load/data/l.java
				com/bumptech/glide/load/data/mediastore/c.java
				com/bumptech/glide/load/data/mediastore/e.java
				com/bumptech/glide/load/engine/DecodeJob.java
				com/bumptech/glide/load/engine/bitmap_recycle/i.java
				com/bumptech/glide/load/engine/bitmap_recycle/j.java
				com/bumptech/glide/load/engine/cache/e.java
				com/bumptech/glide/load/engine/cache/i.java
				com/bumptech/glide/load/engine/executor/a.java
				com/bumptech/glide/load/engine/h.java
				com/bumptech/glide/load/engine/j.java
				com/bumptech/glide/load/engine/p.java
				com/bumptech/glide/load/engine/prefill/a.java
				com/bumptech/glide/load/engine/y.java
				com/bumptech/glide/load/model/c.java
				com/bumptech/glide/load/model/d.java
				com/bumptech/glide/load/model/f.java
				com/bumptech/glide/load/model/s.java
				com/bumptech/glide/load/model/t.java
				com/bumptech/glide/load/resource/a.java
				com/bumptech/glide/load/resource/bitmap/b0.java
				com/bumptech/glide/load/resource/bitmap/c.java
				com/bumptech/glide/load/resource/bitmap/d.java

NO	ISSUE	SEVERITY	STANDARDS	com/bumptech/glide/load/resource/bitmap/l.java Hht6umptech/glide/load/resource/bitmap/m.java com/bumptech/glide/load/resource/bitmap/n.java
2	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/bumptech/glide/load/resource/bitmap/r.java com/bumptech/glide/load/resource/gif/a.java com/bumptech/glide/load/resource/gif/a.java com/bumptech/glide/load/resource/gif/j.java com/bumptech/glide/load/resource/gif/j.java com/bumptech/glide/manager/e.java com/bumptech/glide/manager/f.java com/bumptech/glide/manager/k.java com/bumptech/glide/manager/l.java com/bumptech/glide/manager/l.java com/bumptech/glide/manager/n.java com/bumptech/glide/manager/o.java com/bumptech/glide/manager/o.java com/bumptech/glide/module/d.java com/bumptech/glide/request/singleRequest.java com/bumptech/glide/signature/b.java com/bumptech/glide/signature/b.java com/bumptech/glide/util/pool/a.java com/bumptech/glide/util/pool/a.java com/epic/patientengagement/core/ui/ProgressBar.java com/epic/patientengagement/core/ui/ProgressBar.java com/epic/patientengagement/core/ui/buttons/CoreButto n.java com/epic/patientengagement/core/ui/buttons/CoreButto nUtils.java com/epic/patientengagement/core/ui/bttons/CoreButto nUtils.java com/epic/patientengagement/core/ui/stickyheader/Stick yHeaderAdapter.java com/epic/patientengagement/core/ui/tutorials/PETutoria lFragment.java com/epic/patientengagement/core/utilities/Performance Logger.java com/epic/patientengagement/core/utilities/broadcast/Br oadcastManager.java com/epic/patientengagement/core/webservice/WebServi ceTask.java com/epic/patientengagement/core/webservice/WebServi ceTask.java com/epic/patientengagement/core/webservice/WebServi ceTask.java com/epic/patientengagement/onboarding/views/OrgTer msConditionsView.java com/epic/patientengagement/todo/progress/c.java epic/mychart/android/library/api/classes/WPAPIFirebase

NO	ISSUE	SEVERITY	STANDARDS	MessagingService.java F) டம் Sychart/android/library/appointments/FutureAppoi ntmentFragment.java
				epic/mychart/android/library/appointments/c.java epic/mychart/android/library/customactivities/JavaScript WebViewActivity.java epic/mychart/android/library/customadapters/StickyHea derSectionAdapter/c.java epic/mychart/android/library/general/AccessResult.java epic/mychart/android/library/general/DeepLinkManager. java epic/mychart/android/library/healthlinks/b.java epic/mychart/android/library/healthlinks/b.java epic/mychart/android/library/location/fragments/a.java epic/mychart/android/library/location/services/Appoint mentArrivalService.java epic/mychart/android/library/pushnotifications/CustomF cmListenerService.java epic/mychart/android/library/trackmyhealth/a.java epic/mychart/android/library/ttilities/d0.java epic/mychart/android/library/utilities/e0.java epic/mychart/android/library/utilities/p.java epic/mychart/android/library/utilities/p.java epic/mychart/android/library/utilities/p.java epic/mychart/android/library/utilities/p.java epic/mychart/android/library/utilities/p.java org/mychart/android/library/utilities/p.java org/mychart/android/library/utilities/p.java org/mychart/android/library/utilities/p.java org/mychart/android/library/utilities/p.java org/mm/mynm/v1/clinicalresearch/view/ui/ClinicalTrialsS earchActivity.java org/nm/mynm/v1/finddoctor/api/b.java org/nm/mynm/v1/finddoctor/view/ui/DoctorSearchActivi ty.java org/nm/mynm/v1/findlocation/view/ui/fragment/c.java org/nm/mynm/v1/findlocation/view/ui/fragment/b.java org/nm/mynm/v1/findlocation/view/ui/fragment/b.java org/nm/mynm/v1/findlocation/view/ui/fragment/b.java org/nm/mynm/v1/findlocation/view/ui/fragment/b.java org/nm/mynm/v1/findlocation/view/ui/fragment/b.java org/nm/mynm/v1/findlocation/view/ui/fragment/b.java org/nm/mynm/v1/findlocation/view/ui/GlobalSearchAct ivity.java org/nm/mynm/v1/tooltip/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/epic/patientengagement/homepage/itemfeed/webs ervice/items/ZeroStateFeedItem.java com/epic/patientengagement/todo/models/Questionnair eSeries.java epic/mychart/android/library/utilities/r.java net/bytebuddy/utility/c.java pro/piwik/sdk/d.java
4	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	com/epic/patientengagement/core/pdfviewer/PdfViewM odel.java com/epic/patientengagement/core/utilities/file/FileUtil.ja va com/epic/patientengagement/pdfviewer/pdf/PdfFile.java epic/mychart/android/library/customviews/PdfViewerAct ivity.java epic/mychart/android/library/utilities/k.java net/bytebuddy/agent/ByteBuddyAgent\$AgentProvider\$F orByteBuddyAgent.java
5	MD5 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	epic/mychart/android/library/utilities/k.java pro/piwik/sdk/tools/b.java
6	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	org/nm/mynm/v1/feedback/view/ui/FaqWebViewActivity .java org/nm/mynm/v2/ui/healthbeat/view/HealthBeatActivity .java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/epic/patientengagement/core/utilities/DeviceUtil.jav a com/epic/patientengagement/core/utilities/file/FileChoos erType.java com/epic/patientengagement/core/utilities/file/FileUtil.ja va epic/mychart/android/library/utilities/DeviceUtil.java
8	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/epic/patientengagement/core/utilities/EncryptionUti l.java org/nm/mynm/v1/network/k.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	org/nm/mynm/utils/e.java
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	org/nm/mynm/v1/network/j.java
11	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/epic/patientengagement/core/mychartweb/MyChar tWebViewFragment.java epic/mychart/android/library/prelogin/AccountManagem entWebViewActivity.java
12	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/epic/patientengagement/core/mychartweb/MyChar tWebViewFragment.java

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewFragment.java com/epic/patientengagement/authentication/login/activities/SAMLLoginActivity.java a com/epic/patientengagement/authentication/login/fragments/LongTextDialogFragment.java com/epic/patientengagement/authentication/login/fragments/OrgFragment.java com/epic/patientengagement/authentication/login/utilities/PreloginDeeplinkMana ger.java com/epic/patientengagement/core/extensibility/ExtensibilityLaunchManager.java com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java com/epic/patientengagement/core/utilities/IntentUtil.java com/epic/patientengagement/core/utilities/WebUtil.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/community/WebCommunityManageMyAccountsActivity.java epic/mychart/android/library/customactivities/JavaScriptWebViewActivity.java epic/mychart/android/library/general/DeepLinkManager.java epic/mychart/android/library/general/PeepLinkManager.java epic/mychart/android/library/general/FDlLauncherActivity.java epic/mychart/android/library/general/e.java epic/mychart/android/library/healthlinks/l.java epic/mychart/android/library/healthlinks/l.java epic/mychart/android/library/insurance/e.java

RULE	BEHAVIOUR	LABEL	epic/mychart/android/library/letters/WebLettersActivity.java epic/mychart/android/library/personalize/c.java Epic/mychart/android/library/prelogin/AccountManagementWebViewActivity.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/springboard/CustomFeature.java epic/mychart/android/library/todo/PatientAssignedQuestionnaireWebViewActivity. java epic/mychart/android/library/utilities/CommunityUtil.java epic/mychart/android/library/utilities/k.java epic/mychart/android/library/welcomewizard/WelcomeWizardWebViewFragment Manager.java org/nm/mynm/utils/d.java
			org/nm/mynm/v1/base/SplashActivity.java org/nm/mynm/v1/clinicalresearch/view/ui/ClinicalTrialsDetailActivity.java org/nm/mynm/v1/finddoctor/view/adapter/g.java org/nm/mynm/v2/ui/healthbeat/view/HealthBeatActivity.java org/nm/mynm/v2/ui/login/view/LoginActivity.java org/nm/mynm/v2/ui/settings/view/SettingsActivity.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/epic/patientengagement/authentication/login/activities/PreloginInternalWebVi ewFragment.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/utilities/k.java org/nm/mynm/utils/d.java org/nm/mynm/utils/i.java org/nm/mynm/v2/ui/login/view/LoginActivity.java
00094	Connect to a URL and read data from it	command network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java epic/mychart/android/library/healthlinks/d.java

RULE ID	BEHAVIOUR	LABEL	FILES	
00091	Retrieve data from broadcast collection		com/epic/patientengagement/authentication/login/fragments/LoginFragment.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java epic/mychart/android/library/appointments/FutureAppointmentFragment.java epic/mychart/android/library/billing/PaymentConfirmationActivity.java epic/mychart/android/library/billing/RecentStatementActivity.java epic/mychart/android/library/healthadvisories/HealthAdvisoryMarkCompleteActivity.java epic/mychart/android/library/medications/MedRefillActivity.java epic/mychart/android/library/messages/ComposeActivity.java epic/mychart/android/library/personalize/PersonalizeFragment.java epic/mychart/android/library/springboard/CustomWebModeJumpActivity.java epic/mychart/android/library/testresults/TestResultDetailActivity.java org/nm/mynm/v1/base/BaseActivity.java org/nm/mynm/v1/clinicalresearch/view/ui/ClinicalTrialsViewAllActivity.java org/nm/mynm/v1/fiacalresearch/view/ui/FilterClinicalTrialsActivity.java org/nm/mynm/v1/feedback/view/ui/FavoriteDoctorAndLocationActivity.java org/nm/mynm/v1/feedback/view/ui/FeedbackPatientCareActivity.java org/nm/mynm/v1/fiedback/view/ui/FeedbackSubActivity.java org/nm/mynm/v1/finddoctor/view/ui/FeedbackSubActivity.java org/nm/mynm/v1/finddoctor/view/ui/FleeDoctorActivity.java org/nm/mynm/v1/findlocation/view/ui/FleeDoctorActivity.java	
00202	Make a phone call	control	org/nm/mynm/utils/i.java org/nm/mynm/v2/ui/login/view/LoginActivity.java	
00203	Put a phone number into an intent	control	org/nm/mynm/utils/i.java org/nm/mynm/v2/ui/login/view/LoginActivity.java	
00125	Check if the given file path exist	file	com/epic/patientengagement/core/pdfviewer/PdfFragment.java com/epic/patientengagement/pdfviewer/PdfViewerFragment.java	

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/airbnb/lottie/network/a.java com/airbnb/lottie/network/b.java com/bumptech/glide/disklrucache/a.java com/bumptech/glide/load/c.java com/bumptech/glide/load/model/f.java com/bumptech/glide/load/model/f.java com/epic/patientengagement/pdfviewer/utilities/FileUtils.java epic/mychart/android/library/customobjects/StoredFile.java epic/mychart/android/library/customviews/PhotoViewerActivity.java epic/mychart/android/library/utilities/DeviceUtil.java epic/mychart/android/library/utilities/i.java net/bytebuddy/agent/ByteBuddyAgent\$AgentProvider\$ForByteBuddyAgent.java net/bytebuddy/dynamic/DynamicType.java pro/piwik/sdk/dispatcher/e.java
00036	Get resource file from res/raw directory	reflection	epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/prelogin/WebServer.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/springboard/CustomFeature.java epic/mychart/android/library/utilities/k.java
00089	Connect to a URL and receive input stream from the server	command network	com/airbnb/lottie/network/b.java com/bumptech/glide/load/data/j.java com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/b.java com/bumptech/glide/load/data/j.java com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java
00109	Connect to a URL and get the response code	network command	com/airbnb/lottie/network/b.java com/bumptech/glide/load/data/j.java com/epic/patientengagement/core/webservice/WebServiceTask.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java
00016	Get location info of the device and put it to JSON object	location collection	epic/mychart/android/library/location/models/MonitoredForArrivalAppointment.ja va
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/c.java
00112	Get the date of the calendar event	collection calendar	epic/mychart/android/library/healthlinks/HealthDataSyncService.java epic/mychart/android/library/healthlinks/b.java epic/mychart/android/library/healthlinks/k.java org/nm/mynm/customviewslib/CustomComponentEditText.java
00012	Read data and put it into a buffer stream	file	epic/mychart/android/library/utilities/i.java

RULE ID	BEHAVIOUR	LABEL	FILES	
00022	Open a file from given absolute path of the file	file	com/airbnb/lottie/network/a.java com/airbnb/lottie/network/b.java com/epic/patientengagement/core/utilities/DeviceUtil.java epic/mychart/android/library/customviews/VideoPlayerActivity.java epic/mychart/android/library/messages/Attachment.java net/bytebuddy/android/AndroidClassLoadingStrategy\$Injecting\$Dispatcher\$ForLegacyVm.java	
00024	Write file after Base64 decoding	reflection file	epic/mychart/android/library/messages/Attachment.java	
00108	Read the input stream from given URL	network command	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java epic/mychart/android/library/customobjects/a.java	
00026	Method reflection	reflection	net/bytebuddy/description/type/TypeDescription.java net/bytebuddy/dynamic/loading/ClassInjector.java	
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/b.java com/epic/patientengagement/core/pdfviewer/PdfViewModel.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java	
00032	Load external class	reflection	net/bytebuddy/dynamic/loading/ClassInjector.java	
00046	Method reflection	reflection	net/bytebuddy/dynamic/loading/ClassInjector.java	
00027	Get specific method from other Dex files	reflection	net/bytebuddy/dynamic/loading/ClassInjector.java	
00153	Send binary data over HTTP	http	epic/mychart/android/library/utilities/g.java	
00072	Write HTTP input stream into a file	command network file	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java	

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://mynmbynm.firebaseio.com
App talks to a Firebase database	info	The app talks to Firebase database at https://haiku-push-notifications.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/935722945823/namespaces/firebase:fetch?key=AlzaSyDsx-oLa_G6SUBPetjAl_WjLauJ6n5xWJQ. This is indicated by the response: The response code is 400

***: ::** ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK
Other Common Permissions	3/44	android.permission.CALL_PHONE, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

• OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
20	00011111711201011

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
nm.piwik.pro	ok	IP: 20.121.104.90 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
nm.org	ok	IP: 204.62.118.87 Country: United States of America Region: Illinois City: Chicago Latitude: 41.895187 Longitude: -87.621864 View: Google Map

DOMAIN	STATUS	GEOLOCATION
nmmycharttest.nm.org	ok	IP: 204.62.116.181 Country: United States of America Region: Arkansas City: Little Rock Latitude: 34.746479 Longitude: -92.289589 View: Google Map
play.google.com	ok	IP: 142.250.81.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.w3.org	ok	IP: 104.18.22.19 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
ichart2.epic.com	ok	IP: 199.204.56.101 Country: United States of America Region: Wisconsin City: Madison Latitude: 43.073051 Longitude: -89.401230 View: Google Map

DOMAIN	STATUS	GEOLOCATION
mynmapi.nm.org	ok	IP: 204.62.118.119 Country: United States of America Region: Illinois City: Chicago Latitude: 41.895187 Longitude: -87.621864 View: Google Map
inside.asp	ok	No Geolocation information available.
schemas.datacontract.org	ok	IP: 207.46.197.115 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
www.youtube.com	ok	IP: 142.250.65.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.nm.org	ok	IP: 204.62.118.87 Country: United States of America Region: Illinois City: Chicago Latitude: 41.895187 Longitude: -87.621864 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.epic.com	ok	IP: 13.107.253.71 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
haiku-push-notifications.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
mynm.nm.org	ok	IP: 204.62.118.13 Country: United States of America Region: Illinois City: Chicago Latitude: 41.895187 Longitude: -87.621864 View: Google Map
rex.webqa.epic.com	ok	No Geolocation information available.
www.shareeverywhere.com	ok	IP: 199.204.56.202 Country: United States of America Region: Wisconsin City: Madison Latitude: 43.073051 Longitude: -89.401230 View: Google Map

DOMAIN	STATUS	GEOLOCATION
mynmbynm.firebaseio.com	ok	IP: 35.190.39.113 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
sites.northwestern.edu	ok	IP: 34.199.202.106 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
www.apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
ichart1.epic.com	ok	IP: 204.187.138.40 Country: United States of America Region: Wisconsin City: Verona Latitude: 42.990845 Longitude: -89.568443 View: Google Map

DOMAIN	STATUS	GEOLOCATION
schemas.microsoft.com	ok	IP: 13.107.253.71 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
www.googleapis.com	ok	IP: 142.250.80.42 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
img.youtube.com	ok	IP: 142.251.40.206 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.mychart.org	ok	IP: 13.107.253.71 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
mynmapi.nm.orghttps	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
www.feinberg.northwestern.edu	ok	IP: 23.100.233.65 Country: United States of America Region: Illinois City: Chicago Latitude: 41.850029 Longitude: -87.650047 View: Google Map
xmlpull.org	ok	IP: 185.199.109.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
uat.nm.org	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
releaseofinformation@nm.org mynm@nm.org	org/nm/mynm/v1/feedback/viewmodel/b.java
yourname@example.com example@example.com	Android String Resource



POSSIBLE SECRETS
"firebase_database_url" : "https://mynmbynm.firebaseio.com"
"google_api_key" : "AlzaSyDsx-oLa_G6SUBPetjAl_WjLauJ6n5xWJQ"
"google_crash_reporting_api_key" : "AlzaSyDsx-oLa_G6SUBPetjAl_WjLauJ6n5xWJQ"
"my_chart_password" : "PASSWORD"
"wp_key_preferences_about" : "wp_preference_about"
"wp_key_preferences_allow_all_locales" : "wp_key_preferences_allow_all_locales"
"wp_key_preferences_clear_disc_webview_cache" : "wp_key_preferences_clear_disc_webview_cache"
"wp_key_preferences_clear_ram_webview_cache" : "wp_key_preferences_clear_ram_webview_cache"
"wp_key_preferences_clear_webview_cache" : "wp_key_preferences_clear_webview_cache"
"wp_key_preferences_custom_locale" : "wp_key_preferences_custom_locale"
"wp_key_preferences_custom_phone_book" : "wp_preference_custom_phone_book"
"wp_key_preferences_custom_server" : "wp_preference_custom_server"
"wp_key_preferences_custom_server_switch" : "wp_preference_custom_server_switch"
"wp_key_preferences_enable_webview_cache" : "wp_key_preferences_enable_webview_cache"

POSSIBLE SECRETS "wp_key_preferences_health_connect_switch": "wp_key_preferences_health_connect_switch" "wp_key_preferences_health_data_debug_switch": "wp_key_preferences_health_data_debug_switch" "wp_key_preferences_screenshots": "wp_preference_screenshots" "wp_key_preferences_testing_header": "wp_preferences_testing_header" "wp_key_preferences_tool_tip": "wp_key_preferences_tool_tip" "wp_login_password": "Password" "wp_login_username": "Username" "wp_share_everywhere_dismiss_token_button_title": "Dismiss" "wp_two_factor_authenticate_code_button": "Verify" "wp_two_factor_authentication_success_accessibility_announcement": "Success!" "my_chart_password": "CONTRASEÑA" 0532cfaceb63e9b743b472551dac704e 11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650 16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a 768764bf9ab35c8ccdef1d7fa5ddaefd

POSSIBLE SECRETS

68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166 43812574028291115057151

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

316AD0AA-BF5C-40B4-B41C-26A5486596B1

b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

115792089210356248762697446949407573530086143415290314195533631308867097853951

68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633211138647686124403 80340372808892707005449

c9c6ff9a-8d23-497e-841f-e4094c28e614

POSSIBLE SECRETS

064e6cc7-8875-4dd2-9e3c-d8c8c95b272e

6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

115792089210356248762697446949407573529996955224135760342422259061068512044369



> PLAYSTORE INFORMATION

Title: MyNM by Northwestern Medicine

Score: 2.5512822 Installs: 100,000+ Price: 0 Android Version Support: Category: Medical Play Store URL: org.nm.mobile.myNM

Developer Details: Northwestern Memorial Healthcare, Northwestern+Memorial+Healthcare, None, https://nm.org/mynm, NMGoogleApps@nm.org,

Release Date: Dec 18, 2018 Privacy Policy: Privacy link

Description:

See your medical records, schedule a visit, message your care team, find a healthcare professional, and more with the Northwestern Medicine app for Android. The MyNM app is a secure app for patients powered by MyChart. With MyNM, you can: Manage Your Health: • See your health information and lab results • Securely message your physician and care team. • Schedule new appointments • Request prescription refills • View statements and pay your bill • Track your health and fitness when you enroll in self-tracking programs. Find Care • Search healthcare professionals by specialty, insurance carrier, language preferences, and more. • View profiles for over 4,000 Northwestern Medicine physicians. • See nearby Northwestern Medicine locations, including Emergency Departments and Immediate Care Centers. Access Visitor Resources: • View parking and transportation options • Access hospital maps and view on-site amenities • View nearby hotels and lodging

∷ SCAN LOGS

Timestamp	Event	Error	
		i	

2025-08-28 22:07:02	Generating Hashes	ОК
2025-08-28 22:07:02	Extracting APK	ОК
2025-08-28 22:07:02	Unzipping	ОК
2025-08-28 22:07:03	Parsing APK with androguard	OK
2025-08-28 22:07:04	Extracting APK features using aapt/aapt2	OK
2025-08-28 22:07:04	Getting Hardcoded Certificates/Keystores	OK
2025-08-28 22:07:08	Parsing AndroidManifest.xml	ОК
2025-08-28 22:07:08	Extracting Manifest Data	ОК
2025-08-28 22:07:08	Manifest Analysis Started	ОК
2025-08-28 22:07:08	Reading Network Security config from wp_network_security_config.xml	ОК
2025-08-28 22:07:08	Parsing Network Security config	ОК

2025-08-28 22:07:08	Performing Static Analysis on: MyNM (org.nm.mobile.myNM)	ОК
2025-08-28 22:07:09	Fetching Details from Play Store: org.nm.mobile.myNM	ОК
2025-08-28 22:07:10	Checking for Malware Permissions	ОК
2025-08-28 22:07:10	Fetching icon path	ОК
2025-08-28 22:07:10	Library Binary Analysis Started	ОК
2025-08-28 22:07:10	Reading Code Signing Certificate	ОК
2025-08-28 22:07:10	Running APKiD 2.1.5	ОК
2025-08-28 22:07:15	Updating Trackers Database	ок
2025-08-28 22:07:15	Detecting Trackers	ОК
2025-08-28 22:07:20	Decompiling APK to Java with JADX	ОК
2025-08-28 22:07:41	Converting DEX to Smali	ОК

2025-08-28 22:07:41	Code Analysis Started on - java_source	ОК
2025-08-28 22:07:46	Android SBOM Analysis Completed	ОК
2025-08-28 22:07:48	Android SAST Completed	ОК
2025-08-28 22:07:48	Android API Analysis Started	ОК
2025-08-28 22:07:51	Android API Analysis Completed	ОК
2025-08-28 22:07:52	Android Permission Mapping Started	ОК
2025-08-28 22:07:54	Android Permission Mapping Completed	ОК
2025-08-28 22:07:55	Android Behaviour Analysis Started	ОК
2025-08-28 22:07:59	Android Behaviour Analysis Completed	ОК
2025-08-28 22:07:59	Extracting Emails and URLs from Source Code	ОК
2025-08-28 22:08:06	Email and URL Extraction Completed	ОК

2025-08-28 22:08:06	Extracting String data from APK	ОК
2025-08-28 22:08:07	Extracting String data from Code	OK
2025-08-28 22:08:07	Extracting String values and entropies from Code	ОК
2025-08-28 22:08:12	Performing Malware check on extracted domains	ОК
2025-08-28 22:08:18	Saving to Database	ОК

Report Generated by - MobSF v4.4.0

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.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.