SEKURA
Expertos en seguridad informática

Great Place To Work. Certified

Security Reevaluation and Remediation Validation Report

Evaluación de seguridad realizada a:

BNF

Banco Nacional de Fomento

Periodo de ejecución: 26/09/2024 - 26/09/2024

Fecha de emisión: 26/09/2024

Equipo técnico: Takao Sato, Luis Cuevas

ESTE INFORME ES CONFIDENCIAL: Este documento no debe ser divulgado a terceros, copiado ni reproducido por ningún medio sin la autorización explicita del cliente.

Presentación del informe

Este informe presenta los resultados de la reevaluación de seguridad informática solicitada por **Banco Nacional de Fomento**. El documento está organizado de la siguiente manera: **La sección de confidencialidad** incluye una nota sobre la privacidad del informe y su distribución restringida. En la **introducción**, se explican los **objetivos** del proyecto, su **alcance**, el sistema de puntuación CVSS y los niveles de criticidad, además de las **limitaciones y restricciones encontradas** durante la prueba inicial y la reevaluación.

La **metodología** detalla el enfoque utilizado durante la reevaluación, siguiendo las mismas fases que en la evaluación inicial, incluyendo reconocimiento, análisis de vulnerabilidades corregidas, validación de la explotación y reporte, además de los tipos de pruebas (Black Box). El resumen ejecutivo proporciona una visión general de los hallazgos corregidos y una descripción de las vulnerabilidades mitigadas o pendientes de mitigación.

En el **Objetivo del Proyecto** se establece que el propósito de la reevaluación fue verificar las correcciones aplicadas a las vulnerabilidades previamente identificadas, confirmar la reducción de los riesgos y asegurar que no se introdujeron nuevas vulnerabilidades durante la implementación de las soluciones. Asimismo, se ofrecen recomendaciones adicionales para reforzar la seguridad.

El **Alcance del Proyecto** detalla los límites de la reevaluación, especificando que esta actividad se centró en las mismas aplicaciones y sistemas evaluados previamente, bajo las modalidades de evaluación (blackbox). Se revalidaron los controles de seguridad en las áreas identificadas durante la evaluación inicial.

El **Detalle de Hallazgos** ofrece una tabla que resume los hallazgos previos, indicando su ID, severidad, estado actual (mitigado, en proceso de mitigación, etc.) y una breve descripción. Se proporciona una explicación detallada de cada hallazgo, incluyendo la evidencia de la corrección (capturas de pantalla), impacto residual (CVSS), recomendaciones para futuras mejoras y referencias.

Las **Conclusiones y Resúmenes** presentan los resultados de la reevaluación en una tabla que incluye las vulnerabilidades revisadas y las recomendaciones adicionales, ofreciendo un plan de acción para mantener la seguridad fortalecida. Los apéndices contienen un listado actualizado de las herramientas y tecnologías utilizadas durante la reevaluación, así como una tabla con la lista de verificación de las pruebas realizadas en esta fase. Nuestro trabajo se basó en la verificación de las correcciones aplicadas a las vulnerabilidades conocidas hasta la fecha del informe. No obstante, es importante tener en cuenta que las vulnerabilidades pueden evolucionar con el tiempo, lo que podría afectar las conclusiones de esta reevaluación. Recomendamos que las acciones sugeridas sean evaluadas por la entidad para su implementación continua, ya que contribuirán a fortalecer el marco de control interno informático vigente.

La cantidad de horas utilizadas para la realización de este proyecto ha sido de **10** (diez) horas. Este tiempo incluye todas las etapas del proceso, desde la planificación inicial hasta la entrega final del informe.

Este informe es de uso exclusivo de la Gerencia de Banco Nacional de Fomento y no debe ser presentado, distribuido o referido para ningún otro propósito sin la autorización por escrito de "CORPORATION SEKIURA S.A.C.E.I.".

Estamos a su disposición para cualquier consulta o información adicional y aprovechamos la oportunidad para saludarlo muy atentamente.

Eduardo Lagrave

Chief Operations Officer

Tabla de contenidos

Revisión de historial & Control de versiones 1

Declaración de Confidencialidad y No Divulgación 2

1. Definiciones 2

2. Descargo de Responsabilidad 2

3. Introducción 3

4. Objetivo del Proyecto 3

5. Alcance del Proyecto 3

6. Metodología 3

7. Clasificación de la Severidad: 4

8. Sumario Ejecutivo 6

9. Detalle de hallazgos 7

9.1 Uso de android:requestLegacyExternalStorage="true" 7

9.2 Uso de SDK de Compilación Anticuado 9

9.3 Ejecución en Dispositivos Rooteados 11

9.4 Vulnerabilidad Janus 15

10. Resumen del nivel de seguridad de la aplicación 17

Revisión de historial & Control de versiones

Revision de historial & Control de versiones

Versión	Fecha	Autor	Comentarios
Final	Septiembre 26, 2024	Luis Cuevas	Final
Revisado por		Takao Sato	

Declaración de Confidencialidad y No Divulgación

1. Definiciones

Este documento contiene información confidencial y protegida. Todos los datos proporcionados a Banco Nacional de Fomento se entregan bajo el entendimiento de que no se utilizarán ni divulgarán fuera del contexto de las negociaciones comerciales con CORPORATION SEKIURA SACEI.

El destinatario de este documento se compromete a notificar a los empleados actuales y futuros autorizados a acceder a la información aquí contenida sobre la necesidad de mantener y tratar esta información de acuerdo con la clasificación de este documento.

El destinatario también se compromete a instruir a cada empleado para que no divulgue información relacionada con este documento a terceros, a menos que dicha información sea de dominio público y esté disponible para su uso. Asimismo, el destinatario acuerda no reproducir ni distribuir a terceros cualquier material contenido en este documento sin el consentimiento expreso y por escrito de CORPORATION SEKIURA SACEI.

CORPORATION SEKIURA SACEI se reserva todos los derechos, títulos y la propiedad intelectual sobre el material contenido en este documento, incluyendo toda la información de respaldo, archivos, material de comercialización y multimedia.

Al aceptar este documento, el destinatario acuerda obligarse a cumplir con la declaración antes mencionada.

Información Confidencial: Toda información, ya sea oral, escrita o contenida en cualquier documento, archivo o medio de almacenamiento, designada como confidencial por cualquiera de las partes.

La Contratista: CORPORATION SEKIURA SACEI, que recibe y protege la Información Confidencial proporcionada por La Contratante, comprometiéndose a no divulgarla a terceros.

La Contratante: Banco Nacional de Fomento, que proporciona Información Confidencial a La Contratista y mantiene en todo momento la propiedad de dicha información.

2. Descargo de Responsabilidad

Una prueba de penetración (pentest), es una evaluación que representa un momento específico en el tiempo. Los hallazgos y recomendaciones reflejan las condiciones observadas durante la auditoría y no contemplan cambios posteriores.

Las limitaciones temporales no permiten una evaluación completa de todos los controles de seguridad. La Contratista priorizó la auditoría para identificar los controles de seguridad más vulnerables que podrían ser explotados por un atacante. Se recomienda realizar evaluaciones similares anualmente, ya sea por auditores internos o externos, para asegurar la efectividad continua de los controles.

3. Introducción

Este informe presenta los resultados de la reevaluación de seguridad de seguridad realizado para el Banco Nacional de Fomento. La reevaluación fue llevada a cabo en un ambiente de desarrollo con el fin de verificar las correcciones aplicadas tras la prueba de penetración inicial.

4. Objetivo del Proyecto

El propósito de este proyecto es:

- Verificar si las vulnerabilidades identificadas previamente han sido corregidas adecuadamente.
- Validar que las mitigaciones implementadas cumplen con los requisitos de seguridad establecidos.
- Asegurar que no se hayan introducido nuevas vulnerabilidades durante el proceso de corrección de una vulnerabilidad.

5. Alcance del Proyecto

Esta sección detalla el alcance de la reevaluación de seguridad. La validación de seguridad se limita a la siguiente aplicación corregida:

No.	Activo	Modalidad	Tipo
1	BNF_QA.apk	**Blackbox**	**Externo**

6. Metodología

La reevaluación de seguridad fue llevada a cabo utilizando los mismos estándares y marcos de referencia aplicados en la prueba de penetración inicial, como OWASP y OSSTMM, con el objetivo de verificar las correcciones de las vulnerabilidades previamente identificadas. No se introdujeron nuevas técnicas de evaluación, asegurando la consistencia en la validación.

7. Clasificación de la Severidad:

Rating	CVSS Score
Crítica	9.0 – 10.0
Alta	7.0 – 8.9
Media	4.0 – 6.9
Baja	0.1 – 3.9
Informativa	0.0

Las vulnerabilidades identificadas se agrupan en las siguientes categorías:

Vulnerabilidades Críticas: Estas son debilidades que pueden tener un impacto severo en el sistema, permitiendo a los atacantes tomar control total del sistema, ejecutar código malicioso o acceder a datos altamente sensibles.

Vulnerabilidades Altas: Aunque no tan devastadoras como las críticas, estas vulnerabilidades pueden resultar en daños significativos, incluyendo la exposición de datos sensibles y la interrupción de servicios esenciales.

Vulnerabilidades Medias: Vulnerabilidades que, si bien no representan un riesgo inmediato y grave, pueden ser explotadas en combinación con otras debilidades para comprometer la seguridad del sistema.

Vulnerabilidades Bajas: Problemas menores que no representan una amenaza inmediata pero que, de no ser tratados, podrían ser aprovechados en futuros ataques.

Vulnerabilidades Informativas: Aspectos que no representan una amenaza directa, pero que proporcionan información valiosa sobre el sistema y pueden ser utilizados por atacantes para planificar ataques más sofisticados.

La severidad de los hallazgos identificados se evalúa utilizando el Sistema de Puntuación de Vulnerabilidades Común (CVSS) versión 4.0. Este sistema proporciona un marco estandarizado para evaluar y comunicar la gravedad de las vulnerabilidades de seguridad en sistemas de software, asignando una puntuación entre 0 y 10, donde 10 indica la mayor severidad.

El CVSS considera tres factores principales al calcular la puntuación de una vulnerabilidad:

Impacto de la vulnerabilidad: Incluye las posibles consecuencias de un ataque exitoso, como pérdida de datos, interrupción del sistema o acceso no autorizado. Métricas asociadas: Confidencialidad, Integridad y Disponibilidad.

Explotabilidad de la vulnerabilidad: Considera la complejidad y el esfuerzo necesarios para explotar la vulnerabilidad, así como la probabilidad de éxito de un ataque. Métricas asociadas: Vector de ataque, Complejidad del ataque, Privilegios requeridos e Interacción del usuario.

Alcance de la vulnerabilidad: Evalúa la extensión del impacto de la vulnerabilidad en el sistema o software, determinando si puede ser explotada de forma remota o solo localmente.

Restricciones y Limitaciones

Durante la prueba de penetración, se encontraron varias restricciones y limitaciones que podrían haber afectado los resultados de la evaluación:

Restricciones de tiempo: La evaluación se realizó dentro de un período específico, lo cual limitó la posibilidad de evaluar todos los controles de seguridad.

Acceso limitado: Durante la ejecución del pentest, se crearon dos cuentas de acceso para realizar las pruebas correspondientes. Sin embargo, al cabo de algunas horas, estas cuentas dejaron de ser accesibles a través de la aplicación, lo que impidió su recuperación y uso en las pruebas posteriores. Este inconveniente se presentó en un contexto de tiempo limitado para la realización del pentest, debido a notificaciones y requerimientos adicionales por parte del cliente, lo que restringió aún más la capacidad de realizar un análisis exhaustivo.

Adicionalmente, la página web o aplicación web de prueba, a la que debía acceder la aplicación móvil bajo evaluación, presentó problemas de disponibilidad recurrentes. Las constantes caídas de esta plataforma interrumpieron repetidamente el análisis y los procedimientos planificados para la auditoría de seguridad, afectando significativamente la calidad y la profundidad de las pruebas de penetración.

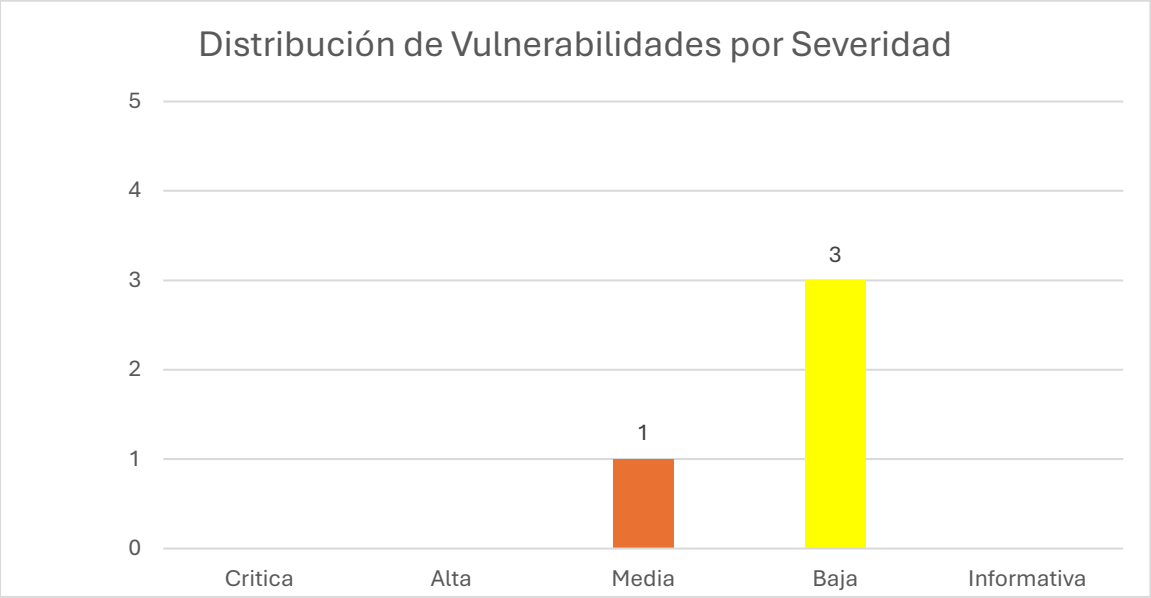
Estos inconvenientes, tanto en la accesibilidad de las cuentas de prueba como en la disponibilidad de la plataforma web, limitaron la capacidad del equipo para llevar a cabo un pentest completo. Como resultado, la evaluación de seguridad no pudo cubrir todas las áreas planeadas, lo que podría haber dejado posibles vulnerabilidades sin identificar.

8. Sumario Ejecutivo

Este documento presenta un resumen ejecutivo correspondiente a la reevaluación (RE-TEST) del trabajo realizado para Banco Nacional de Fomento, que se llevó a cabo entre el 23/sep/2024 y 28/sep/2024. El objetivo de la presente reevaluación (RE-TEST) es validar la presencia (persistencia) o no (mitigación) de las vulnerabilidades previamente identificadas y asegurar que no persisten riesgos de seguridad en las aplicaciones evaluadas.

Durante la reevaluación de seguridad, se verificaron un total de 4 (cuatro) vulnerabilidades previamente identificadas, categorizadas según su severidad utilizando el Sistema de Puntuación de Vulnerabilidades Común (CVSS) versión 4.0.

A continuación, se presenta una gráfica que muestra la distribución de las vulnerabilidades encontradas según su severidad:



Impacto de las vulnerabilidades encontradas

Vulnerabilidad	Severidad	Impacto	Estado Actual
Uso de android:requestLegacyExternalStorage="true"	Medio	Exposición de datos sensibles a aplicaciones no confiables	Mitigado
Uso de SDK de Compilación Anticuado	Bajo	Riesgo de incompatibilidades y falta de parches de seguridad	Mitigado
Ejecución en Dispositivos Rooteados	Bajo	Aumento de la superficie de ataque y posibles compromisos de seguridad	Mitigado
Vulnerabilidad Janus	Bajo	Manipulación de aplicaciones legítimas para introducir código malicioso	Mitigado

9. Detalle de hallazgos

En esta sección se presentan en detalle los hallazgos obtenidos durante la reevaluación de seguridad, incluyendo capturas de pantalla que respaldan cada uno de los hallazgos verificados. Cada hallazgo se describe con precisión, proporcionando información sobre la vulnerabilidad evaluada, su impacto potencial y las recomendaciones para garantizar su mitigación efectiva.

9.1 Uso de android:requestLegacyExternalStorage="true"

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:L/VA:N/SC:H/SI:H/SA:N

Puntuación: 5.3

Severidad: Medio

El uso de *android:requestLegacyExternalStorage="true"* permite a la aplicación continuar utilizando el almacenamiento externo de manera heredada, lo cual ignora las restricciones de seguridad mejoradas introducidas en Android 10. Esta configuración puede llevar a la exposición de datos sensibles a aplicaciones no autorizadas, permitiendo la lectura y modificación de información almacenada en almacenamiento externo sin las debidas restricciones de seguridad. Durante la revisión del archivo AndroidManifest.xml, se identificó que esta configuración está habilitada, lo cual representa un riesgo significativo de fuga de información y de corrupción de datos. Esta configuración no solo expone datos sensibles, sino que también incumple con las recomendaciones de seguridad actuales de Android.

APK	Componente vulnerable	Estado
BNF_QA.apk	AndroidManifest.xml	**Mitigado**

```
1   ersionCodename="14" package="py.com.itti.bnf.qa" platformBuildVersionCode="34" platformBuildVersionName="14">
50  QA] BNF" android:name="android.app.Application" android:requestLegacyExternalStorage="true">
51
52
53
54
55
56
57
58
59
60
61
62
63  oid:exported="true" android:hardwareAccelerated="true" android:launchMode="singleTop" android:name="py.com.itti.bnf
64
```

Screen 1. Estado anterior

```
AndroidManifest.xml
50  <application android:appComponentFactory="androidx.core.app.CoreComponentFactory" android:extractNativeLibs="false" android:
    icon="@mipmap/launcher_icon" android:label="[QA] BNF" android:name="android.app.Application" android:
    requestLegacyExternalStorage="false">
51      <receiver android:exported="false" android:name="com.dexterous.flutterlocalnotifications.ScheduledNotificationReceiver"/>
52      <receiver android:exported="false" android:name="com.dexterous.flutterlocalnotifications.ScheduledNotificationBootReceiver
        ">
53          <intent-filter>
```

Screen 2. Estado actual

Recomendaciones

- Migrar la aplicación para que utilice Scoped Storage, siguiendo las mejores prácticas de seguridad recomendadas por Android.
- Implementar mecanismos de encriptación para cualquier dato sensible almacenado en el almacenamiento externo.
- Realizar revisiones de seguridad regulares y pruebas de penetración para asegurar que la aplicación cumple con las normativas actuales de seguridad.
- Deshabilitar el uso de requestLegacyExternalStorage y refactorizar el código para usar APIs seguras de manejo de archivos.

Referencias

- https://developer.android.com/training/data-storage
- https://developer.android.com/about/versions/10/privacy/changes#scoped-storage

9.2 Uso de SDK de Compilación Anticuado

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:N/VA:N/SC:N/SI:N/SA:L

Puntuación: 2.3

Severidad: Bajo

La aplicación está configurada para utilizar un minSdkVersion=23, lo cual permite que se ejecute en dispositivos con Android 6.0 (Marshmallow) o versiones superiores. Aunque la aplicación utiliza un compileSdkVersion=34 y un targetSdkVersion=34, lo que le permite beneficiarse de las últimas mejoras y parches de seguridad introducidos en Android 13, la configuración en el minSdkVersion permite la ejecución en versiones más antiguas del sistema operativo que no cuentan con las mismas capacidades de seguridad. Esto aumenta el riesgo de exposición a vulnerabilidades que han sido mitigadas en versiones posteriores de Android. Las versiones modernas de Android introducen mejores prácticas de gestión de permisos y mejoras en la protección de datos que no están disponibles en Android 6.0.

APK	Componente vulnerable	Estado
BNF_QA.apk	AndroidManifest.xml	**Mitigado**

```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="8" android:versionName="1.0.0" android:compileSdkVersion="34" android:compileSdkVersionCodename="14" package="py.com.it
  xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-sdk android:minSdkVersion="23" android:targetSdkVersion="34" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
    <uses-permission android:name="android.permission.CAMERA" />
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW" />
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <uses-permission android:name="android.permission.WAKE_LOCK" />
    <uses-permission android:name="android.permission.VIBRATE" />
    <uses-permission android:name="android.permission.USE_BIOMETRIC" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" android:maxSdkVersion="28" />
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.ACCESS_MEDIA_LOCATION" />
    <queries>
```

Screen 3. Estado anterior

```
1.  <?xml version="1.0" encoding="utf-8"?>
2.  <manifest android:versionCode="14" android:versionName="1.0.0" android:compileSdkVersion="34" android:compileSdkVersionCodename="14" package="py.com.itti.bnf.qa"
3.    xmlns:android="http://schemas.android.com/apk/res/android">
4.      <uses-sdk android:minSdkVersion="24" android:targetSdkVersion="34" />
5.      <uses-permission android:name="android.permission.INTERNET" />
6.      <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
7.      <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
8.      <uses-permission android:name="android.permission.CAMERA" />
9.      <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW" />
10.     <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
11.     <uses-permission android:name="android.permission.WAKE_LOCK" />
12.     <uses-permission android:name="android.permission.VIBRATE" />
13.     <uses-permission android:name="android.permission.USE_BIOMETRIC" />
14.     <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" android:maxSdkVersion="28" />
15.     <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
```

Screen 4. Estado actual

Recomendaciones

- Considerar elevar el minSdkVersion a al menos 24 (Android 7.0, Nougat) para aprovechar las mejoras de seguridad implementadas en esta versión y posteriores.
- Evaluar el impacto de esta actualización en la base de usuarios, considerando la adopción de dispositivos y versiones de Android.

- Mantenerse al día con las actualizaciones de seguridad y mejores prácticas recomendadas por Android para minimizar los riesgos de seguridad futuros.

Referencias

- https://developer.android.com/about/versions/nougat/android-7.0-changes
- https://developer.android.com/tools/releases/platforms

9.3 Ejecución en Dispositivos Rooteados

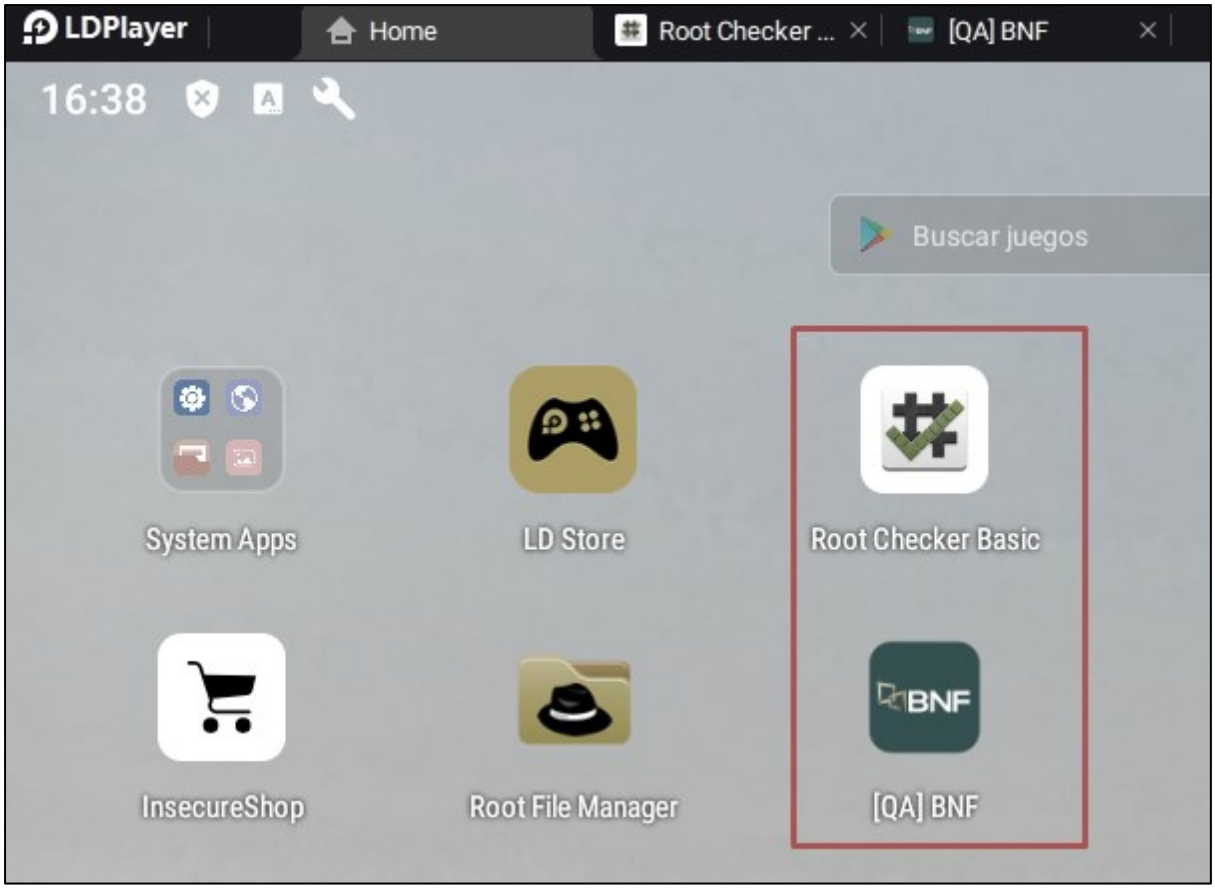
CVSS: 4.0/AV:N/AC:L/AT:P/PR:H/UI:P/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L

Puntuación: 2.0

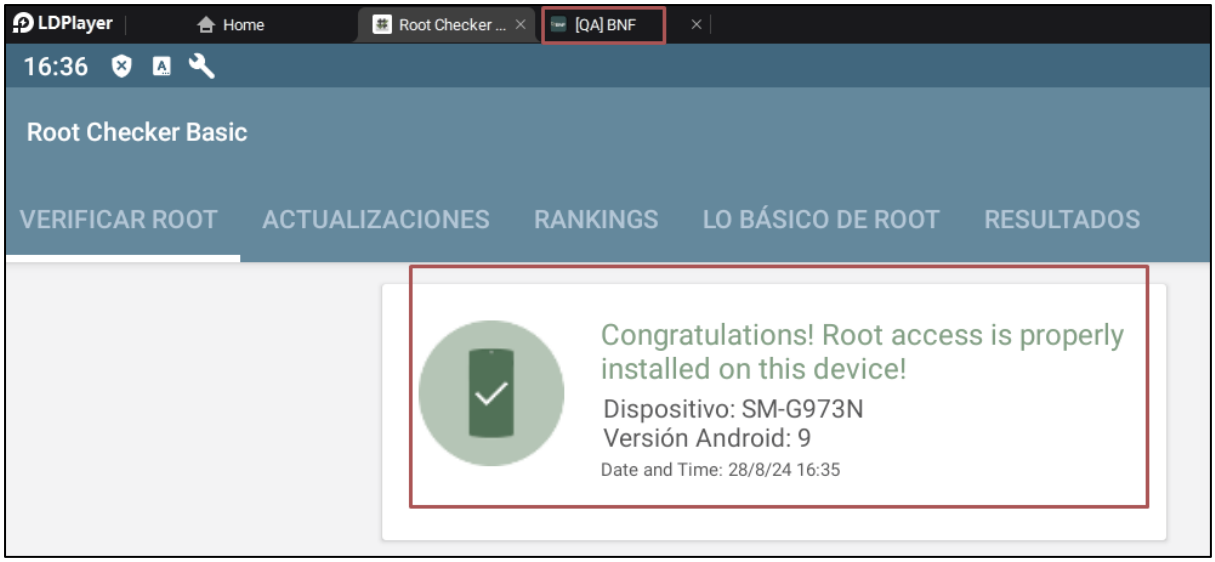
Severidad: Bajo

Se ha detectado que la aplicación [QA] BNF puede ser ejecutada en dispositivos con acceso root habilitado, lo cual fue verificado utilizando la herramienta "Root Checker Basic" en un dispositivo con Android 9. Esta condición implica un riesgo significativo, ya que en dispositivos rooteados, aplicaciones maliciosas o usuarios no autorizados pueden obtener permisos de superusuario, permitiendo el acceso y la modificación de archivos de sistema protegidos. Esto expone a la aplicación a posibles manipulaciones, acceso a datos sensibles, y desactivación de funciones de seguridad críticas. La posibilidad de ejecución en un entorno comprometido, como es el caso de los dispositivos con root, incrementa el riesgo de exposición de información sensible y de instalación de malware, comprometiendo así tanto la seguridad de la aplicación como la de sus usuarios.

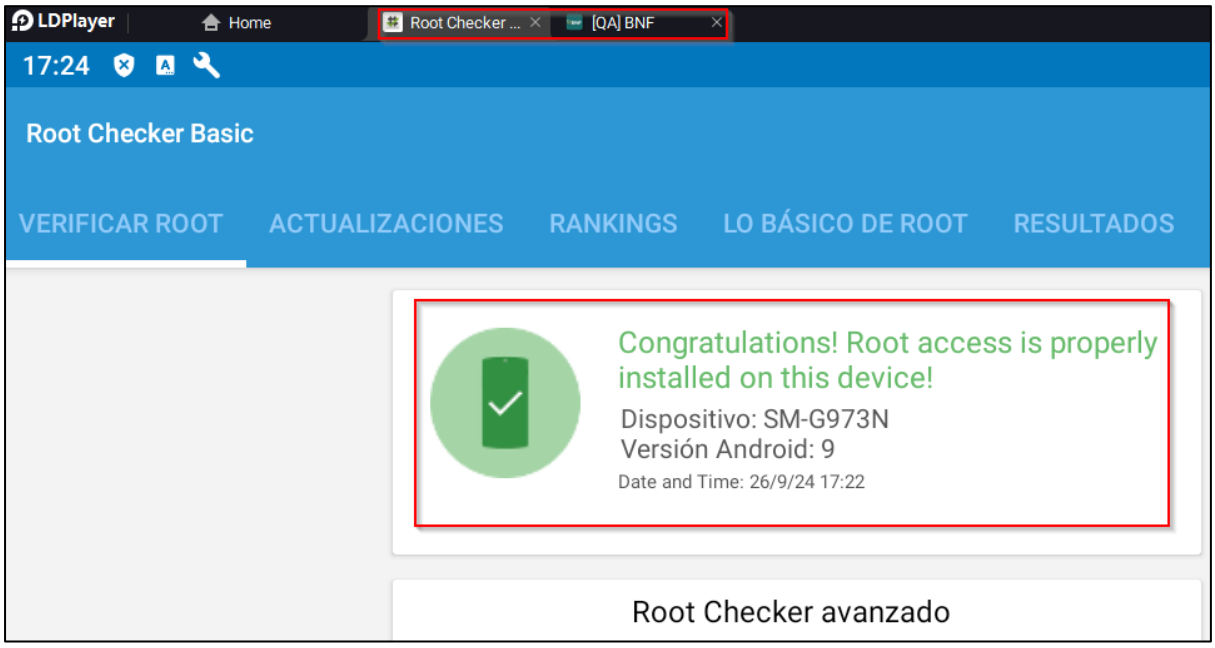
APK	Estado
BNF_QA.apk	**Mitigado**



Screen 5. Estado anterior

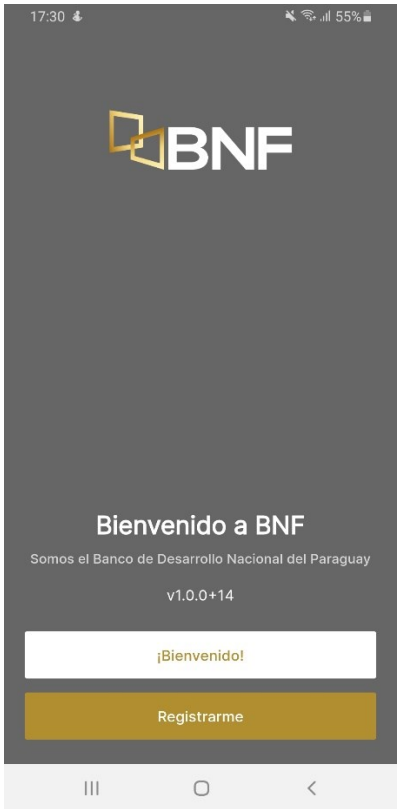


Screen 6. Estado anterior



Screen 7. Estado actual (aun puede instalarse en dispositivos root)

Screen 8. Estado actual (sin embargo, la aplicación no se puede ejecutar en dispositivos root ya que este permanece en esta manera y no permite logear)



Screen 9. Estado actual (en equipos no root si podemos ejecutar correctamente la aplicación e intentar registrarnos)

Recomendaciones

- Implementar detección de root en la aplicación para alertar a los usuarios sobre los riesgos de ejecutar en un dispositivo rooteado.
- Deshabilitar funciones críticas o limitar el acceso a datos sensibles cuando se detecte que la aplicación está siendo ejecutada en un entorno con root.
- Utilizar técnicas de encriptación para proteger datos sensibles, de modo que incluso si se accede a ellos, permanezcan inaccesibles sin la clave correcta.
- Instruir a los usuarios sobre los riesgos de seguridad de usar dispositivos rooteados y promover el uso de dispositivos sin modificaciones para acceder a la aplicación.

Referencias

- https://developer.android.com/privacy-and-security/security-tips#RootedDevice
- https://developer.android.com/privacy-and-security/security-tips#DetectingRoot
- https://source.android.com/docs/security

9.4 Vulnerabilidad Janus

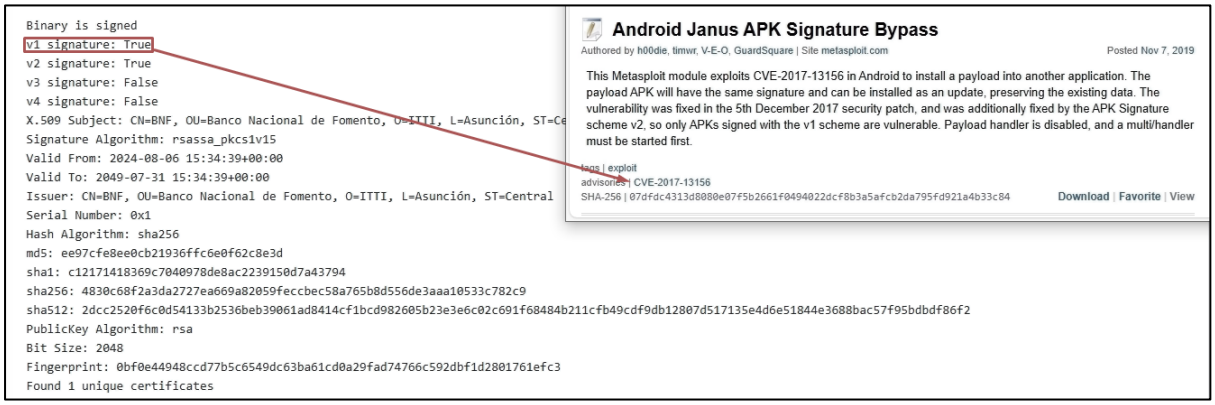
CVSS: 4.0/AV:N/AC:L/AT:P/PR:H/UI:P/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L

Puntuación: 2.0

Severidad: Bajo

Se ha identificado que la aplicación BNF_QA.apk está firmada utilizando el esquema de firma APK v1, lo que la hace vulnerable a la explotación de la vulnerabilidad conocida como Janus (CVE-2017-13156). Esta vulnerabilidad permite a un atacante modificar el contenido de un archivo APK sin invalidar su firma digital. En concreto, al firmar el APK con el esquema v1, un atacante podría inyectar código malicioso en el APK sin alterar su integridad percibida, lo que permitiría la instalación del APK modificado sin alertar al sistema operativo de Android. La explotación de esta vulnerabilidad puede resultar en la ejecución de código malicioso, robo de datos sensibles, y comprometer la seguridad del dispositivo y la aplicación.

APK	Estado
BNF_QA.apk	**Mitigado**



Screen 10. Estado anterior

Screen 11. Estado actual

Recomendaciones

- Actualizar el esquema de firma de la aplicación a al menos APK Signature Scheme v2 o v3 para protegerse contra la vulnerabilidad Janus y mejorar la seguridad de la aplicación.
- Realizar un nuevo ciclo de pruebas para asegurar que la aplicación funciona correctamente con los esquemas de firma actualizados.
- Implementar un proceso regular de revisión y actualización de las políticas de firma para garantizar el uso de las mejores prácticas de seguridad.
- Considerar la implementación de medidas adicionales de seguridad, como la verificación de integridad de código y análisis de comportamiento anómalo para detectar intentos de explotación.

Referencias

- https://developer.android.com/about/versions/nougat/android-7.0-changes#apk_signature_v2
- https://source.android.com/docs/security/features/apksigning
- https://packetstormsecurity.com/files/155189/Android-Janus-APK-Signature-Bypass.html

10. Resumen del nivel de seguridad de la aplicación

Para determinar el nivel general de seguridad de la aplicación móvil, se consideran varios factores, incluyendo la cantidad y gravedad de las vulnerabilidades encontradas, la efectividad de las medidas de mitigación implementadas y la sensibilidad de los datos y sistemas involucrados.

Nivel Muy Bajo: Existen múltiples y graves vulnerabilidades que requieren acciones inmediatas para proteger la aplicación móvil. El riesgo de explotación es muy alto.

Nivel Bajo: Hay vulnerabilidades graves que requieren mejoras urgentes en la seguridad. El riesgo de explotación es alto.

Nivel Medio: Se han encontrado algunas vulnerabilidades de gravedad moderada y se necesitan mejoras en las medidas de seguridad. Existe un riesgo moderado de explotación.

Nivel Alto: Se han identificado pocas vulnerabilidades de baja gravedad y las medidas de mitigación son efectivas. La seguridad es sólida y el riesgo de explotación es bajo.

Nivel Muy Alto: Casi no hay vulnerabilidades significativas y la seguridad es excelente. El riesgo de explotación es mínimo.

Nivel de Seguridad General