

تقرير متابعة حول فحص أمني لتطبيق تعليم عن بعد بعد التحديث

مقدمة :

بعد تسليم التقرير الأمني الأول الخاص بمشكلة تسريب المحتوى في التطبيق ، تم تسليم الثغرات (black-box testing) للمطورين لمعالجتها. وبعد تنفيذ التحديثات، طُلب إجراء فحص أمني جديد للتأكد من فعالية الحماية الحالية. يهدف هذا التقرير إلى تقييم الحماية بعد التحديث وتحديد ما إذا تم فعلاً سد الثغرات السابقة أو ظهور ثغرات جديدة.

نقاط الفحص وتقييم النتائج :

(Developer Mode) التلاعب بوضع المطور

- محاولة تفعيل وضع المطور أثناء تشغيل التطبيق بهدف إعادة تنفيذ سيناريو :الوصف .التلاعب القديم
- فشل جميع المحاولات لتفعيل وضع المطور أثناء التشغيل، مما يدل على نجاح :النتيجة .آلية الحماية الجديدة

2. Root تشغيل التطبيق في بيئة:

- للتحقق من آليات root تم اختبار تشغيل التطبيق على أجهزة تمتلك صلاحيات :الوصف .كشف الروت
- ، وتم تسجيل Root تم تشغيل التطبيق على بعض الأجهزة بنجاح رغم وجود :النتيجة الشاشة دون أي إنذار أو منع. وهذا يُظهر وجود ثغرة في آلية التحقق من صلاحيات الروت أو نقص في شمولية الحماية عبر مختلف الأجهزة

3. تشغيل التطبيق على إصدارات أندرويد قديمة:

- Android 10 التحقق مما إذا كان التطبيق ما زال يعمل على إصدارات أقل من :الوصف
- نجاح التحديث في منع تشغيل التطبيق على الإصدارات القديمة، ما ساهم في سد :النتيجة ثغرات سابقة كانت ممكنة فقط على هذه الأنظمة

4. (Watermarking) آلية العلامات المائية:

- فحص وجود علامة مائية متحركة تحتوي على معرف المستخدم أثناء عرض :الوصف الفيديوهات، لضمان تتبع أي تسريب

- حتى الآن، مما يبقى المحتوى غرضة watermark لم يتم تطبيق نظام: النتيجة
- للتسريب دون إمكانية التتبع للمستخدم المسؤول.

5. فحص تسجيل الشاشة بعد التحديث:

- محاولة إعادة سيناريو تسجيل الشاشة باستخدام أدوات خارجية بعد التحديث: الوصف
- بسبب توقف دعم الإصدارات القديمة، لم تنجح الطريقة السابقة في تسجيل: النتيجة
- المحتوى، مما يعني نجاح التحديث في هذا الجانب

6. ثغرة إضافية (خارج نطاق التقرير الحالي):

- تم رصد مشكلة جديدة لم تكن ضمن نطاق الفحص الحالي: الوصف
- يمكن تقديم تقرير منفصل بخصوص هذه الثغرة حسب طلب العميل: الملاحظة

التوصيات:

1. لتغطي أكبر عدد ممكن من الأجهزة Root تعزيز آلية اكتشاف صلاحيات الـ
2. (User ID) ديناميكي يظهر بشكل متحرك ويحتوي على معرف المستخدم Watermark تطبيق نظام
3. لتتبع أي حالة تسريب محتوى (ID)
4. Android 10 الاستمرار في تطبيق قيود التشغيل على الإصدارات الأقدم من
5. تقديم فحص إضافي بناءً على الثغرة المكتشفة خارج النطاق

الخاتمة:

يُظهر الفحص أن التحديث الأخير للتطبيق قد نجح في سد عدد من الثغرات السابقة، لا سيما المرتبطة بوضع المطور وتسجيل الشاشة على الأجهزة القديمة. إلا أن بعض الجوانب الأمنية مثل اكتشاف صلاحيات الروت ونظام العلامة المائية لم تُعالج بعد بشكل كافٍ، وتبقى بحاجة إلى تدخل إضافي لتعزيز الحماية.

Reported by : Mostafa Nassar

Date : 18 APR 2025

Report NO.2

App Name : Hidden info