Bewertungsbericht für Gruppe 9: Next-Intent Vulnerability

Florian Hansen Michael Frank

19. Dezember 2020

Die Gruppe 9 hat sich mit der Arbeit von [1] beschäftigt, welche die Schwachstellen (NIVs) in öffentlichen und privaten `Intents` des Android-Betriebssystems behandelt. Kurz zusammengefasst ist der Text verständlich, wir sehen jedoch in seiner Form sowie im Inhalt Verbesserungsbedarf. Die Ausarbeitung der Gruppe 9 erhält von uns **7 von 10 Punkten**. Im Folgenden begründen wir die Bewertung.

Im gesamten Text findet man eine Mischung von englischen und deutschen Fachbegriffen, wie beispielsweise die Formulierung *„Diese spezifische Vulnerability betrifft allerdings [...]“*. Die Einhaltung einer Sprache erscheint uns als angemessener und wissenschaftlicher. Zudem haben wir diverse Fehler in der Grammatik feststellen können. Auch dies trägt nicht gerade zur Lesbarkeit bei. Ein Beispiel hierfür ist die Formulierung aus Abschnitt 2 *„So könnte es z.B. passieren, dass ein/e Angreifer*in beim Betrachten der Appstruktur eine öffentlich zugängliche Komponente detektiert, die Variablen an eine private Komponente übergibt“*. Wie man in dem Beispiel und in anderen Abschnitten sieht, werden oft umgangssprachliche Gebilde wie *„kleine Applikationen“* verwendet. „Klein“ kann in diesem Kontext alles bedeuten. Ob damit die Anzahl der Zeilen der Codebasis, die Anzahl an Schwachstellen, die Speichergröße, die Popularität oder die Einfachheit einer Anwendung gemeint ist, ist nicht klar und muss vermutet werden. **Aufgrund der genannten Kritikpunkte ziehen wir der Gruppe einen halben Punkt ab.**

Der Inhalt des Textes ist grundsätzlich verständlich, jedoch fühlt man sich an einigen Stellen etwas verlassen. Es werden diverse Fachwörter verwendet, ohne sie auch nur im Ansatz zu erläutern. So ist der Satz *„Eine dieser Sicherheitslücken*

ist die Next-Intent Vulnerability, welche die Kommunikation zwischen Android Applikationen als Angriffspfad verwendet.“ unverständlich, da der Leser nicht genau weiß, was „Angriffspfad“ bedeutet. Auch wird dieser Begriff in den folgenden Absätzen nicht erläutert, sodass die Schwachstelle nicht richtig verstanden werden kann. Im selben Zusammenhang werden auch Begriffe wie *„öffentliche Activities“* verwendet, ohne diese zu behandeln. Wie dann die Kommunikation und die damit verbundene Schwachstelle funktioniert, wird hier nicht klar. Es wird auch häufig auf die *„Struktur einer Applikation“* referenziert und damit versucht, Schwachstellen zu erläutern. Jedoch wird dies nirgends definiert bzw. erläutert, sodass auch hier vermutet werden muss, um was es sich handelt. Auch im vierten Abschnitt „Auswertung“ hätten wir uns etwas mehr Tiefe gewünscht. Es wird zum Beispiel nicht ganz klar, wie die Zahl „100%“ zustande gekommen ist. Es ist bspw. interessant, ob es sich im Testlauf um eine einzelne Gruppe handelte, welche die manuellen und automatisierten Tests durchführten, oder ob zwei voneinander unabhängige Gruppen gewählt wurden. Die einzelne Gruppe kann unter Umständen von den vorherigen Tests beeinflusst worden sein. Auch wenn die Tiefe des Inhalts darunter leidet, lernt man dennoch einiges über die Wichtigkeit beim Umgang mit `Intents` und Werkzeugen, die Schwachstellen detektieren. **Wir ziehen der Gruppe ein und halb Punkte aufgrund von fehlenden Definitionen und Erläuterungen ab, die den Inhalt unverständlich und oberflächlich gestalten.**

Als nächstes sind uns fehlende Quellenangaben aufgefallen. Zu Beginn der Arbeit werden alle Quellen einmal genannt. In den Folgeabschnitten ist jedoch nicht mehr ganz klar, auf welche Quelle sich gerade bezogen wird. Man könnte bspw. vermuten, dass sich die restlichen Abschnitte fälschlicherweise auf die zuletzt genannte Quelle beziehen. Gerade in dem Abschnitt 4 „Auswertung“ könnte man fälschlicherweise annehmen, dass es sich dabei um die Ergebnisse der Gruppe selbst und nicht einer ihrer Quellen handelt. Aufgrund des Kontextes war uns bewusst, dass sich die Kapitel auf die von Ihnen bearbeitete Ausarbeitung beziehen, dennoch wären Quellenangaben auch in Folgeabschnitten, bspw. am Ende eines Absatzes, angebracht gewesen. **Wir ziehen der Gruppe dafür einen Punkt ab, da Quellen hauptsächlich nur im ersten Abschnitt „Kontext“ genannt werden.**

Die beschriebene Planung für die praktische Demonstration der Sicherheitslücke erachten wir als gut und sinnvoll, wir haben diesem Ansatz nichts auszusetzen.

Die Bewertungskategorien mit Gewichtungen und Abzügen waren wie folgt:

Verständlichkeit (50%)	**3.5 von 5.0**
Methodik und Tiefe (25%)	**1.0 von 2.5**
Arbeitsplanung (25%)	**2.5 von 2.5**

Literatur

[1] M. A. El-Zawawy, E. Losiouk, and M. Conti. Do not let next-intent vulnerability be your next nightmare: type system-based approach to detect it in android apps. *International Journal of Information Security*, März 2020.