NACHRICHTEN
Österreich
17. Juli 2025

Alarmstufe Rot! So gefährdet die "TapTrap"-Attacke Ihre Android-Apps!

Sicherheitsforscher der TU Wien warnen vor "TapTrap"-Attacken, die 76% der Android-Apps gefährden. Sensible Daten in Gefahr!

Seattle, USA - In einer alarmierenden Entwicklung haben Sicherheitsforscher der TU Wien eine neue Angriffsmethode mit dem Namen „TapTrap“ entdeckt, die potenziell eine große Anzahl von Android-Apps gefährdet. Diese Technik wurde kürzlich auf der Sicherheitskonferenz USENIX in Seattle vorgestellt und betrifft über 76% der rund 100.000 untersuchten Anwendungen im Google Play Store. Der Angriff erlaubt es bösartigen Apps, das Berechtigungssystem von Android zu umgehen und ohne das Wissen der Nutzer auf sensible Daten zuzugreifen oder schädliche Aktionen auszuführen. Philipp Beer von der TU Wien erläutert, dass besonders die eingebauten

Animationsübergänge des Systems ausgenutzt werden, um eine täuschend echte Benutzeroberfläche zu schaffen.

Die Attacke erfolgt ohne spezielle Berechtigungen, wodurch die schädlichen Apps beim Download harmlos erscheinen. In Tests wurde nachgewiesen, dass es Angreifern möglich ist, innerhalb eines kurzen Zeitfensters von 3 bis 6 Sekunden unbemerkt auf kritische Berechtigungen wie die Kamera oder das Mikrofon zuzugreifen. Bei einer Benutzerstudie konnten die meisten Teilnehmer die Angriffe nicht erkennen; nur 21% bemerkten Sicherheitsindikatoren, wenn auf die Kamera zugegriffen wurde.

Angriffsvektoren und Risiken

Die Forscher identifizierten mehrere gefährliche Angriffszenarien, darunter:

- Berechtigungsumgehung: Zugang zu Kamera, Mikrofon und Standort ohne Einverständnis.
- Benachrichtigungsinterzeption: Zugriff auf wichtige Benachrichtigungen, beispielsweise Zwei-Faktor-Authentifizierungscodes.
- Geräteerasure: Vollständiges Löschen des Geräts durch Manipulation des Nutzers.
- Web-Schwachstellen: Clickjacking-Angriffe gegen verbreitete Browser wie Chrome und Firefox.

Die Möglichkeiten sind vielschichtig und das Forschungsteam warnte, dass theoretisch sogar schädliche Aktionen wie das Starten von Banking-Apps oder das Löschen sämtlicher Daten auf einem Gerät durchgeführt werden könnten.

Schutzmaßnahmen und Status

In Bezug auf die Sicherheit haben Browser wie Firefox und Google Chrome bereits Maßnahmen ergriffen, um diese Lücke zu schließen. Google hat jedoch kein festes Datum für umfassende systemweite Sicherheitsupdates bereitgestellt, um das Risiko für

Nutzer auf Android-Version 15 zu minimieren. Zudem wurde die Schwachstelle mit zwei CVEs (CVE-2025-3067 für Chrome und CVE-2025-1939 für Firefox) gekennzeichnet und Google verlieh den Forschern eine Belohnung von 10.000 USD für ihre Entdeckung.

Google hat im aktualisierten **Android Security Paper 2023** betont, wie wichtig starke Sicherheitsmaßnahmen im Umgang mit mobilen Geräten sind. Cyberkriminalität ist ein wachsendes Problem, und 2022 wurden über 800.000 Beschwerden beim FBI eingereicht, wobei die Verluste 10 Milliarden Dollar übertrafen. Das Papier beschreibt die Notwendigkeit einer engen Zusammenarbeit zwischen Entwicklern, Geräteherstellern und Sicherheitsforschern, um Plattformanfälligkeiten zu erkennen und zu beseitigen.

Facebook-Nutzer müssen wachsam bleiben und untrustwürdige Quellen meiden. Zudem sollten Nutzer in den Einstellungen unter „Bedienungshilfen“ die App-Animationen deaktivieren, um sich einen gewissen Schutz zu verschaffen. Entsprechend den Testergebnissen bleibt jedoch abzuwarten, wie schnell Google und andere Anbieter auf diese bedenkliche Sicherheitslage reagieren werden.

Details	
Vorfall	Cyberkriminalität
Ort	Seattle, USA
Quellen	• **www.kleinezeitung.at** • **cybersecuritynews.com** • **blog.google**