Sicherheitsrisiko WLAN-Calling: Updates nach Schwachstellen entdeckt

Eine Sicherheitslücke bei WLAN-Calling betrifft weltweit 140 Millionen Nutzer, insbesondere in Österreich, Brasilien und Russland.

Die Entwicklung der Mobiltechnologie hat in den letzten Jahren erhebliche Fortschritte gemacht. Eine der bemerkenswertesten Innovationen ist das WLAN-Calling, welches seit 2016 verfügbar ist und es ermöglicht, Anrufe über WLAN-Verbindungen statt über das Mobilfunknetz herzustellen. Diese Technologie erweist sich als besonders vorteilhaft in Gebieten mit schwacher Mobilfunkabdeckung, wie in Tunneln oder unterirdischen Räumen.

Schwachstellen bei der Sicherheit

In einer aktuellen Untersuchung hat das **Cispa Helmholtz-Zentrum für Informationssicherheit** in Saarbrücken grave Sicherheitslücken in der Technologie des WLAN-Calling aufgedeckt. Adrian Dabrowski, einer der Forscher, wies darauf hin, dass der sichere Verbindungsaufbau zwischen Smartphones und Mobilfunknetzen nicht für alle Anbieter gewährleistet ist.

Besonders besorgniserregend ist, dass 13 von 275 analysierten Mobilfunkanbietern aus Ländern wie Österreich, Slowakei, Brasilien und Russland von dieser Sicherheitslücke betroffen sind. Diese Schwachstelle stellt die Kommunikationssicherheit für etwa **140 Millionen Kunden** in Frage, die potenziell abgehört werden konnten.

Ursachen der Sicherheitsproblematik

Die Gründe für diese unsichere Kommunikation liegen vor allem in unzureichenden Verschlüsselungsstandards. Sowohl die Mobilfunkanbieter als auch die Smartphone-Hersteller müssen laut Dabrowski und seinem Team in die Pflicht genommen werden, um die Sicherheit der Nutzer zu gewährleisten. Auch Sicherheitsbehörden könnten möglicherweise Zugriff auf die betroffenen Kommunikationsdaten erhalten haben, was die Problematik noch verstärkt.

Betroffene Technologien und Updates

Ein weiterer Fokus der Untersuchung lag auf Chips des taiwanesischen Herstellers **MediaTek**, die in vielen Android-Smartphones, unter anderem von Herstellern wie **Xiaomi**, **Oppo**, **Realme** und **Vivo**, verbaut sind. Diese Chips wiesen ebenfalls Schwachstellen auf, die bei gezielten Angriffen ausgenutzt werden konnten, um die Verschlüsselung der Geräte auf eine schwächere Variante herabzusetzen.

Die Forscher konnten jedoch nicht genau bestimmen, wie viele Nutzer weltweit von potenziellen Angriffen betroffen waren. Dennoch gab es mittlerweile Sicherheitsupdates, die zur Behebung dieser Schwachstellen implementiert wurden, um die Nutzer zu schützen.

Wichtigkeit der Aufklärung

Die Enthüllungen rund um die Sicherheitslücken beim WLAN-Calling zeigen, wie kritisch der Schutz der Kommunikation in der digitalen Welt geworden ist. Es ist entscheidend, dass sowohl Verbraucher als auch Anbieter die Risiken verstehen, die mit der Nutzung solcher Technologien verbunden sind. Eine transparente Kommunikation über Sicherheitsrisiken und Umsetzungsmaßnahmen sollte von den Mobilfunkanbietern zur obersten Priorität erklärt werden, um das Vertrauen der Nutzer

nicht zu gefährden.

Über die Thematik der Sicherheitslücken berichtete auch SR info im Radio am 31.07.2024, was auf die Dringlichkeit aufmerksam macht, diese Probleme schnellstmöglich zu lösen.

- **NAG**

Details

Besuchen Sie uns auf: n-ag.de